UNIVERZITET SINGIDUNUM

Milan Milosavljević
Vladislav Miškovic

ELEKTRONSKA TRGOVINA

BEOGRAD, 2011.

UNIVERZITET SINGIDUNUM

Prof. dr Milan Milosavljević
Doc. dr Vladislav Miškovic

ELEKTRONSKA TRGOVINA

Prvo izdanje

Beograd, 2011.

ELEKTRONSKA TRGOVINA

Autori:
Prof. dr Milan Milosavljević
Doc. dr Vladislav Miškovic

Recenzenti:
Prof. dr Mladen Veinović
Prof. dr Branko Kovačević

Izdavač:
UNIVERZITET SINGIDUNUM
Beograd, Danijelova 32

Za izdavača:
Prof. dr Milovan Stanišić

Tehnički urednik:
Novak Njeguš

Dizajn korica:
Aleksandar Mihajlović

Godina izdanja:
2011.

Tiraž:
500 primeraka

Štampa:
Mladost grup
Loznica

ISBN: 978-86-7912-338-1

PREDGOVOR

Udžbenik Elektronska trgovina je prevashodno namenjen studentima studijskog programa Marketing i trgovina na Departmanu za poslovnu ekonomiju Univerziteta Singidunum. Po svome sadržaju i načinu izlaganja, predstavlja pogodnu dodatnu literaturu za sve studijske programe na Univerzitetu koji se dotiču nekog aspekta savremene elektronske trgovine kao globalnog fenomena. Izbor materijala i način prezentovanja je delom rezultovao iz višegodišnjeg iskustva autora u predavanjima i vežbama iz predmeta Elektronske poslovne komunikacije sa studijskog programa Poslovna informatika. Ovo iskustvo je pomoglo da se na adekvatan način prenesu osnovne postavke tehnološke infrastrukture savremene elektronske trgovine studentima čije je usmerenje u društveno ekonomskom polju.

Udžbenik se sastoji od deset poglavlja koja pokrivaju sve relevantne aspekte elektronske trgovine, od platnih sistema, poslovnih modela, tehnološke infrastrukture, preko marketinških i komunikoloških aspekata, do najznačajnijih servisa bezbednosti koji omogućavaju siguran protok novčanih sredstava i vrednosti na javnoj komunikaciono računarskoj mrežni kakav je internet.

Poglavlja 1, 2, 5, 6, 9 i 10 napisao je prof. Milan Milosavljević, dok su poglavlja 3, 4, 7 i 8 napisana od strane doc.Vladislava Miškovica.

Autori izražavaju posebnu zahvalnost Rektoru Univerziteta Singidunum prof. Milovanu Stanišiću i Prorektoru prof. Miloradu Unkoviću, za podršku i podsticaj da se ovaj projekat završi u planiranom roku.

Autori se takodje zahvaljuju recenzentima, prof. Mladenu Veinoviću i prof. Branku Kovačeviću, na korisnim sugestijama.

U Beogradu, 4.02.2011.god. *Autori*

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

SADRŽAJ

1. OSNOVE ELEKTRONSKE TRGOVINE

1.1 UVOD

Elektronska trgovina (e-commerce, e-trgovina) u savremenoj razvijenoj formi nije bila poznata pre 1995. godine. Nepodeljeno je mišljenje da se njenim početkom može smatrati pojava prvog sajta elektronske trgovine, Amazon.com [1]. Priča o Amazon.com, najpoznatijoj kompaniji za e-trgovinu u SAD, odražava u velikoj meri i priču o e-trgovini u celini. Ideje o Amazonu su nastale 1994. godine, kada je Jeff Bezos, tada 29 godišnji stariji zamenik predsednika u D. E. Shaw, investicionoj banci sa Vol Strita, pročitao da je korišćenje Interneta raslo po stopi od 2300 % godišnje. Za Bezosa, taj podatak je ukazivao na izvanrednu priliku. Napustio je dotadašnji posao i počeo da istražuje koje bi proizvode mogao uspešno da prodaje onlajn posredstvom Interneta. Izbor je pao na knjige. Sa preko tri miliona naslova u štampi u bilo koje vreme, ni jedna fizička knjižara ne bi mogla imati u prodaji više od malog procenta te količine. Virtuelna knjižara bi mogla ponuditi potencijalno kompletnu svetsku produkciju. Uporedna dinamika objavljivanja knjiga, distribucije i maloprodajne industrije, takođe su bili povoljni. Sa preko 2500 izdavača u SAD, i dva najveća prodavca na malo, Barnes and Noble i Borders, koji su obavljali svega 12 % od ukupne prodaje, na tržištu nisu postojali dominantni igrači, koji bi svakog malog početnika brzo eliminisali. Postojanje dva velika distributera, Ingram Books i Baker and Taylor, značilo je da bi Amazon morao da skladišti samo minimalan inventar. Bezos je lako prikupio nekoliko miliona dolara od privatnih investitora i u julu 1995. Amazon.com je počeo sa poslovanjem na mreži. Amazon je nudio kupcima četiri privlačna razloga da tamo obavljaju kupovinu: *izbor* (baza podataka od 1.1 milion naslova), *udobnost* (kupovati bilo kada, bilo gde, sa pojednostavljenim naručivanjem po Amazonovoj patentiranoj "1-klik" tehnologiji ekspresne kupovine), *cena* (visoki popusti za bestselere) i *usluga* (podrška kupcima elektronske pošte, i putem telefona, automatizovano potvrđivanje naručivanja, informacije o praćenju i slanju robe, i td).

Uspon Amazona je bio izuzetan. Januara 1996., Amazon se preselio iz kancelarije od 35 kvadratnih metara u skladište od 1600 kvadratnih metara. Do kraja 1996.-e, Amazon je imao skoro 200.000 kupaca. Njegovi prihodi su se popeli na 15,6 miliona $, ali je kompanija objavila ukupni gubitak od 6,24 miliona $. U maju 1997., Amazon je postao javna firma, prikupljajući 50 miliona $ kapitala. Njegovi početni dokumenti o javnoj ponudi su ukazivali na nekoliko načina na koje je Amazon očekivao da ostvari nižu troškovnu strukturu u poređenju sa tradicionalnim knjižarama – ne bi morao da investira u skupe maloprodajne nekretnine, imao bi umanjenu potrebu za osobljem i ne bi morao da drži obiman inventar, jer se u velikoj meri oslanjao na distributere knjiga.

U 1998., Amazon je proširio proizvodnu liniju, prvo dodajući muzičke CD-ove, a zatim i video i DVD izdanja. Amazon nije više bio zadovoljan samo prodavanjem knjiga: njegova poslovna strategija je sada bila "da postane najbolje mesto za kupovinu, pronalaženje i otkrivanje *bilo kog proizvoda i usluge* dostupnih onlajn". Prihodi za tu godinu su već dostigli $610 miliona, ali su se gomilali i gubici, učetvorostručujući se na $125 miliona.

Sl.1.1.1 Originalna prva stranica Web sajta Amazon.com iz 1995. godine, sa čijom pojavom se može računati početak doba savremene elektronske trgovine.

Prekretnica u razvoju Amazona bila je 1999.-a godina. Bezos je najavio da je cilj za Amazon da postane "Najveća zemaljska prodavnica". U februaru, Amazon je pozajmio preko 1 milijardu dolara, koristeći fondove da finansira proširenje i pokrije operativne gubitke. Tokom godine, u liniju proizvoda su dodati elektronika, igračke, proizvodi za domaćinstvo, softver i video igre. Takođe je uvedeno i nekoliko mesta za trgovinu, uključujući Amazon.com Auctions (aukcije, slične onim ponuđenim od eBay), zShops (onlajn izlozi za male prodavce na malo), kao i sothebys.amazon.com, zajednički poduhvat sa aukcijskom kućom Sotheby's. Da bi održavao nove linije proizvoda, Amazon je značajno proširio svoje kapacitete za skladištenje i disitribuciju, dodajući 8 novih distributivnih centara, koji su obuhvatali približno 370.000 kvadratnih matara. Do kraja 1999., Amazon je više nego udvostručio svoje prihode u odnosu na 1998.-u, beležeći prodaju od $1,6 milijardi. Ali u isto vreme, Amazonovi gubici nisu pokazivali nikakve znakove snižavanja, dostižući $720 miliona za tu godinu.

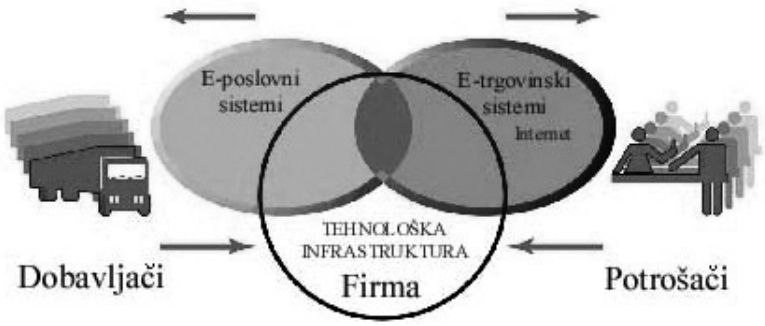
Godina 2000. je okončana sa sasvim drugačijim rezultatima od 1999. godine. Cena akcija je značajno pala u odnosu na vrhunac iz decembra 1999, kada su vredele $113,00 po akciji. To je bila godina kolapsa .com kompanija. Ovim se završava takozvana I era u razvoju elektronske trgovine, karakterisana izuzetno brzim rastom, širokom rasprostranjenošću reklamiranja na Web-u i tehnološki uslovljenim profitom. II era u razvoju elektronske trgovine počinje 2001. godine konsolidacijom poslovanja, pre svega u pravcu uvođenja mešovitih modela poslovanja (klik i brik, odnosno elektronsko i klasično) i tradicionalnih izvora finansiranja u uslovima novih zakonskih regulativa. Tehnološki zasnovan profit zamenjuje poslovno orjentisan profit. Amazon je preživeo krah .com kompanija. Godišnji prihodi su porasli, zahvaljući proširivanju prodajnog asortimana i inostranoj prodaji sa $3.9 milijardi u 2002. na $10.7 milijardi u 2006. godini. U decembru 2008. godine Amazon je dobio S&P 100 indeks, a u martu 2010. godine je imao veću tržišnu vrednost od Target Corporation, Home Depot, Costco, Barnes and Noble, i Best Buy Samo je Walmart između Američkih klasičnih trgovinskih lanaca imao veću vrednost od Amazona.

1.2 OSNOVNA SVOJSTVA E-TRGOVINE

Danas, samo petnaestak godina kasnije, imamo podatak da je na planetarnom nivou u 2008. godini 875 miliona ljudi kupovalo online, što predstavlja porast od oko 40% u poslednje dve godine. Važno je uočiti da brz rast i promene koje su se dogodile u prvih desetak petnaest godina e-trgovine predstavljaju samo početak. 21. vek će biti doba digitalno omogućenog društvenog i poslovnog života, čiju skicu danas samo možemo naslućivati [2]. Postoje procene da će celokupna planetarna trgovina do 2050 godine biti e-trgovina. Da bi smo dobili sliku o ovom novom globalnom fenomenu, neophodno je da prvo definišemo osnovne pojmove.

Pod e-trgovinom podrazumevaćemo trgovinske transakcije između organizacija i pojedinaca, zasnovane na digitalnoj tehnologiji. U ovom određenju, pođednaku važnost imaju obe komponente: digitalne tehnologije, koje se prevashodno odnose na Internet i Web kao i trgovina, koja podrazumeva razmenu vrednosti (tj. novca) za robe i usluge izvan individualnih i organizacionih granica [3].

Postoji posebna debata između specijalista i akademskih sredina koje se bave e-trgovinom u vezi odnosa između elektronske trgovine i elektronskog poslovanja. Po jednima elektronska trgovina obuhvata celokupnu elektronski podržanu aktivnost jedne organizacije, uključujući i sveukupnu infrastrukturu njnog informacionog sistema. Druga strana u ovoj raspravi zastupa stav da e-poslovanje obuhvata sve interne i eksterne elektronski podržane aktivnosti jedne organizacije uključujući i e-trgovinu. Imajući u vidu definiciju elektronske trgovine u kojoj presudnu ulogu ima razmena vrednosti izvan granica jedne organizacije, što nije primarna odlika elektronskog poslovanja, bliži smo stavu da elektronsko poslovanje u opštem slučaju ne obuhvata elektronsku trgovinu. Preciznije, e-poslovne aplikacije se transformišu u e-trgovinu onda kada se u okviru njih pojavljuje razmena vrednosti. Kompleksan odnos e-trgovine i e-poslovanja je ilustrovan na Sl.1.2.1.



Sl.1.2.1 Elektronska trgovina dominantno obuhvata transakcije koje prelaze granice poslovnih organizacija

Pojava elektronske trgovine predstavlja pravu revoluciju u poslovanju, ne samo po do sada neviđenoj superiornoj tehnološkoj osnovi zasnovanoj na modernim telekomunikacijama, računarstvu, informacionim tehnologijama i kriptologiji. Pre ere e- trgovine marketing i prodaja proizvoda su se oslanjali na masovni neusmereni marketing i radnu snagu i umeće neposrednih prodavaca. Potrošači su posmatrani kao pasivni ciljevi reklamnih kampanja, koje menjaju dugoročno odnos kupca prema datom proizvodu i trenutno utiču na njegove kupovne navike. Potrošač je bio zarobljen geografskim i socijalnim barijerama, ograničen na uski lokalni krug u potrazi za najboljim odnosom cena

– kvalitet. Informacije o cenama, troškovima i taksama su mogle biti skrivene od kupaca, omogućavajući formiranje profitabilne tzv. informacione asimetrije u korist prodajnih organizacija. Ovde ćemo pod informacionom asimetrijom podrazumevati svaki disparitet u relevantnim tržišnim informacijama koje dele učesnici u nekoj transakciji.

Elektronska trgovina je dovela u pitanje tradicionalno poslovno mišljenje. Stoga je od važnosti da ukratko analiziramo jedinstvena svojstva tehnologije elektronske trgovine, pri čemu se ova jedinstvenost fiksira dominantno u odnosu na tradicionalne metode trgovine i poslovanja. Navešćemo sedam ključnih svojstava e-trgovine koje je čine jedinstvenim i globalnim fenomenom savremenog poslovanja.

1.2.1. Sveprisutnost

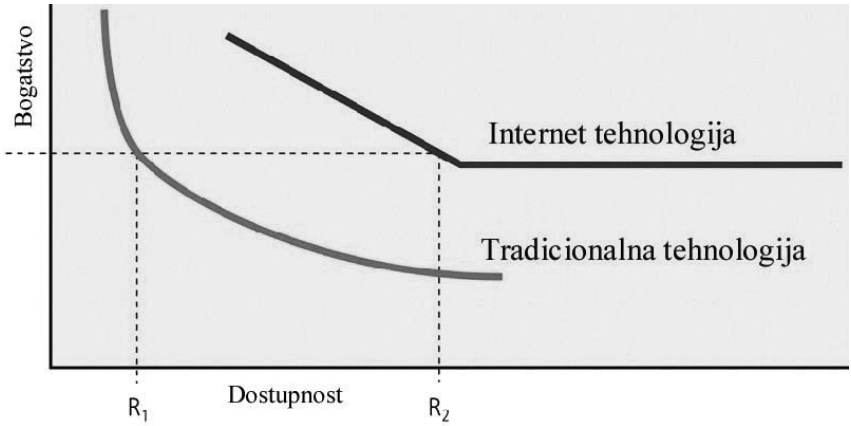
U tradicionalnoj trgovini, tržište je fizičko mesto na kome se obavljaju transakcije. Sveprisutnost elektronske trgovine znači njenu prisutnost bez ikakvih fizičkih i vremenskih ograničenja. Trgovinu je moguće obavljati sa personalnog računara iz kuće, sa posla, iz automobila i td. Sa stanovišta kupca, sveprisutnost znači redukciju cene transakcija, odnosno u opštijem razmatranju redukciju tzv. kognitivne energije, odnosno mentalne energije potrebne za obavljanje transakcije.

1.2.2. Globalni zahvat

Tehnologija e-trgovine omogućava da prevazilaženjem geografskih, vremenskih, kulturoloških i nacioanlnih barijera, veličina tržišta e-trgovine bude potencijalno jednaka celokupnoj svetskoj on-line populaciji, koja je u 2010.godine iznosila oko 1,97 milijardi korisnika, što predstavlja oko 28,7% od ukupne svetske populacije od oko 6,85 milijardi ljudi [4].

1.2.3. Univerzalni standardi

Tehnički standardi Interneta, na kojima se dominantno zasniva e-trgovina su univerzalni standardi, zajednički za sve nacije i sve državne zajednice na planeti. Ovim se znatno snižavaju tzv. pristupni trškovi tržištu, odnosno cena koju prodavci moraju platiti da bi izneli svoje proizvode na jedno tržište. Univerzalni standardi snižavaju i cenu pretrage tržišta, tj. napor koji treba napraviti da bi se na tržištu pronašla adekvatna ponuda. Kreiranjem jedinstvenog, sveobuhvatnog svetskog tržišta na kome se opis i cena prouzvoda mogu jednostavno i jeftino prezentovati svim učesnicima trgovine, nalaženje najpovoljnije cene jednog proizvoda postaje jednostavno, brzo i jeftino. Tehnologija elektronskog trgovanja prvi put u istoriji obezbeđuje lako nalaženje svih dobavljača, cena i uslova dostave zadatog proizvoda bilo gde u svetu.



Sl.1.2.2. Zavisnost informacionog bogatstva i dostupnosti za tradicionalne i Internet tehnologije. IZVOR: Evans and Wurster, 1997.

1.2.4. Informaciono bogatstvo

Informaciono bogatstvo se odnosi na kompleksnost i sadržajnost neke poruke. Tradicionalno tržište, oslonjeno na klasične maloprodajne prodavnice poseduje veliko informaciono bogatstvo, koje obezbeđuje personalizovanu prodaju licem u lice, uz sve prigodne audiovizuelne znake. Informaciono bogatstvo tradicionalnog tržišta, čini ga izuzetno snažnim tržišnim okruženjem. Pre razvoja Weba postojao je trade-off između informacionog bogatstva i dostupnosti. Što je veći auditorijum dostupan, poruke koje im se mogu uputiti su informaciono siromašnije, videti sl.1.2.2.

1.2.5. Interaktivnost

Tehnologije e-trgovine su interaktivne u smislu dvosmernog komuniciranja između prodavca i kupca. Interaktivnost omogućava on-line prodavcu angažovanje kupca slično onom koje se postiže prodajom lice u lice, ali na znatno globalnijoj i masovnijoj osnovi.

1.2.6. Informaciona gustina

Pod informacionom gustinom ćemo podrazumevati ukupnu količinu i kvalitet informacija dostupnih svim učesnicima na tržištu. Internet i Web tehnologije znatno uvećavaju informacionu gustinu. Uz redukciju cene prikupljanja, memorisanja, obrade i prenosa informacija, ove tehnologije istovremeno povećavaju protok, tačnost i dostupnost informacija, čineći ih korisnijim i značajnijim više nego ikad do sada. Ovo je dalje rezultovalo

u bogatstvu, niskoj ceni i visokom kvalietu dostupnih informacija. Povećanje informacione gustine dovelo je do niza promena u poslovanju. Na elektronskom tržištu, cene i troškovi su postali mnogo transparentniji. Od povećanja informacione gustine imaju koristi i prodavci. On-line prodavci mogu saznati sada mnogo više podataka o kupcima, što im omogućava segmentaciju tržišta na grupe koje su u stanju da plate različitu cenu za isti proizvod.

1.2.7 Personalizacija-kastomizacija

Personalizacija je usmeravanje marketinških poruka na imenovane pojedince, uz adaptaciju poruka tako da sadrže uvažavanje njihovih interesa, procenjenih na osnovu prikupljenih podataka o prošlim kupovinama. Nove tehnologije omogućavaju i kastomizaciju, odnosno promenu isporučenih proizvoda ili servisa u skladu sa korisnikovim preferencijalima, ponašanju ili eksplicitno izraženim željama. Uz interaktivnu prirodu tehnologije e-trgovine, veliki broj informacija o potrošačima može biti prikupljen u trenutku obavljanja trgovine. Sa porastom gustine informacija, veliki broj informacija o potrošačevim prethodnim kupovinama i ponašanju može biti uskladišten i korišćen od strane onlajn trgovaca. Rezultat je nivo personalizacije i prilagođavanja zahtevima koji je nezamisliv uz postojeće trgovinske tehnologije. Na primer, ono što gledamo na televiziji možemo oblikovati jednostavnim izborom kanala, ali ne možemo menjati sadržaj kanala koji je izabran. Nasuprot tome, *Wall Street Journal Online* omogućava da se izabere tip novosti koje pretplatnik želi da vidi na prvoj stranici kada pristupi elektronskoj verziji ovih novina [5].

E-trgovina i digitalna tržišta koje ona stvara, obećavaju da će se ostvariti neke korenite, do sada neviđene promene u trgovini. Jedna od tih promena, na primer, verovatno će biti i veliko smanjenje informacione asimetrije među svim učesnicima na tržištu (potrošačima i trgovcima). U prošlosti, trgovci i proizvođači su bili u mogućnosti da spreče potrošače u saznavanju o njihovim troškovima, strategijama cenovnih diskriminacija i profitima od prodaje. Ovo postaje teže ostvarivo kod e-trgovine, i ukupno tržište potencijalno će postati više cenovno konkurentno. S druge strane, jedinstvene dimenzije tehnologije e-trgovine nabrojane u Tabeli 1.2.1 takođe ukazuju na mnoge nove mogućnosti marketinga i prodaje. Skup interaktivnih, personalizovanih i bogatih poruka postaje ostvarljivo isporučivati segmentiranim, ciljnim potrošačkim grupama. Tehnologije e-trgovine omogućavaju trgovcima da znaju mnogo više o potrošačima i da koriste ove informacije efektivnije nego što je to ikad bilo moguće u prošlosti. Da bi stvari bile još složenije, ove iste tehnologije omogućavaju trgovcima da znaju o ostalim trgovcima više nego što je to ikad ranije bilo moguće.

U Tabeli 1.2.1. sumarno je prikazano svih sedam karakteristika e - trgovine, uporedo sa njihovim poslovnim značajem.

SEDAM JEDINSTVENIH OSOBINA TEHNOLOGIJE E-TRGOVINE	
DIMENZIJA TEHNOLOGIJE E-TRGOVINE	POSLOVNI ZNAČAJ
Sveprisutnost – Internet/ mrežna tehnologija je dostupna svuda: na poslu, kod kuće, i na drugim mestima, preko mobilnih uređaja, u bilo koje vreme	Tržište se proširuje van tradicionalnih granica i uklonjeno je sa vremenske i geografske lokacije. "Tržišni prostor" (marketspace) je stvoren; kupovina se može dogoditi bilo kada. Pogodnosti za potrošača su poboljšane, troškovi kupovine su sniženi
Globalna dostupnost – Tehnologija prelazi nacionalne granice, širom planete	Trgovina je omogućena van kulturnih i nacionalnih granica bez ikakvih izmena. "Tržišni prostor" potencijalno uključuje milijarde potrošača i milione preduzeća, širom sveta
Univerzalni standardi – Postoji jedan skup tehnoloških standarda, naime, Internet standarda	Postoji jedan skup tehničkih i medijskih standarda širom sveta
Bogatstvo – Video, audio i tekstuelne poruke su moguće	Video, audio i tekstuelne marketinške poruke su uključene u pojedinačnu marketing poruku i potrošačko iskustvo
Interaktivnost – Tehnologija funkcioniše kroz interakciju sa korisnikom	Potrošači su uključeni u dijalog koji dinamički prilagođava iskustvo samom pojedincu i čini potrošača učesnikom u procesu isporuke dobara tržištu
Gustina informacija – Tehnologija snižava informacione troškove i podiže kvalitet	Troškovi obrade i skladištenja informacija i troškovi komunikacije su značajno sniženi, dok se opticaj, tačnost i blagovremenost značajno poboljšavaju. Informacije postaju obilne, jeftine i precizne
Personalizacija / Prilagođavanje zahtevima – Tehnologija dozvoljava da personalizovane poruke budu isporučene kako pojedincima tako i grupama	Personalizacija marketinških poruka i prilagođavanje proizvoda i usluga zahtevima zasnovanim na osobinama pojedinca

Tabela 1.2.1 Sedam jedinstvenih svojstava tehnologije e - trgovine

1.3. VRSTE ELEKTRONSKE TRGOVINE

Postoji veliki broj različitih tipova elektronske trgovine, koje se mogu kategorisati na različite načine. Mi ćemo se držati podele koja uvažava prirodu tržišnih odnosa, odnosno ko je prodavac, a ko kupac. U tabeli 1.3.1 dat je sumaran pregled 5 najčešćih vrsta e – trgovine.

GLAVNE VRSTE E-TRGOVINE	
VRSTE E-TRGOVINE	PRIMER
B2C – Business to Consumer, Preduzeće ka Potrošaču	Amazon.com je opšti prodavac koji prodaje potrošačke proizvode, kupcima u maloprodaji
B2B – Business to Business, Preduzeće ka Preduzeću	eSteel.com je berza industrije čelika koja nudi elektronsko tržište proizvođačima i kupcima čelika
C2C – Consumer to Consumer, Potrošač ka Potrošaču	eBay.com nudi tržišni prostor gde potrošači mogu licitirati ili direktno prodavati robu drugim potrošačima
P2P – Peer to Peer, Pojedinac ka Pojedincu	Gnutella je softverska aplikacija koja omogućava potrošačima da međusobno razmenjuju muziku, bez uplitanja stvaraoca tržišta kao u C2C e-trgovini
M-trgovina, Mobilna trgovina	Bežični mobilni uređaji, kao PDA (personal digital assistant, lično digitalno pomagalo) ili mobilni telefoni, mogu biti korišćeni za obavljanje trgovinskih transakcija

Tabela 1.3.1. Glavne vrste e-trgovine

1.3.1. B2C (Business to Consumer) e-trgovina

Najčešći oblik e-trgovine u kome on-line preduzeća pokušavaju da privuku individualne kupce. Iako je udeo B2C srazmerno mali u ukupnoj e-trgovini, oko 230 milijardi $ u 2010.godini, iskazuje konstantni eksponencijalni rast od pojave 1995. godine [6]. U okviru B2C postoji niz podkategorija, kao što su portali, on-line prodavnice, provajderi sadržaja, transakcioni brokeri, kreatori tržišta i provajderi usluga.

1.3.2. B2B (Business to Business) e-trgovina

B2B elektronska trgovina, u kojoj preduzeća trguju sa drugim preduzećima, najveća je forma elektronske trgovine, sa oko 3 800 milijardi $ transakcija u 2010. godini. U istoj godini je ukupna trgovina ovog tipa, bez obzira na tehnološku osnovu iznosila oko 15 000

milijardi $, tako da elektronska komponenta ovog tipa trgovanja ima izuzetan potencijal rasta, [6]. Dominantna vrsta B2B elektronske trgovine se odnosi na razmene između preduzeća, mada su se razvili i drugi oblici trgovine, kao što je e-distributerstvo, B2B servis provajderi, mačmarkeri, infomedijatori i td.

1.3.3. C2C (Consumer to Consumer) e-trgovina

U ovom tipu elektronske trgovine individualni kupci vrše direktnu međusobnu kupoprodaju, uz pomoć marketmejkera, kao što je npr. sajt eBay.com. U ovom tipu trgovine potrošač priprema proizvod za tržište, stavljajući ga na aukciju ili prodaju, uz oslanjanje na market mejkera u formiranju kataloga proizvoda, obezbeđivanju alata za pretragu, kao i kompletiranje transakcije, naplate i dostave.

1.3.4. P2P (Peer to Peer) tehnologija

Peer to peer tehnologija omogućava Internet korisnicima razmenu fajlova i tračunarskih resursa direktno, bez posrednika ili nekog centralnog Web servera. Npr. Gnutella je peer to peer softverska aplikacija koja omogućava korisnicima direktnu razmenu muzičkih sadržaja, po pravilu bez ikakvih naplata. Počev od 1999. godine preduzetnici i investitori su pokušali da različite aspekte tehnologije pojedinac-ka-pojedincu e-trgovini. Napster.com, koji je osnovan radi pomaganja Internet korisnicima u pronalaženju i onlajn razmeni MP3 muzičkih fajlova, možda je najpoznatiji primer P2P e-trgovine. U 2000. godini, Recording Industry of America, trgovinska organizacija najvećih kompanija za snimanje, uspešno je tužila Napster za narušavanje zakona o pravima kopiranja, dozvoljavanjem članovima Napstera da razmenjuju autorski zaštićene muzičke numere bez nadoknade nosiocima autorskih prava.

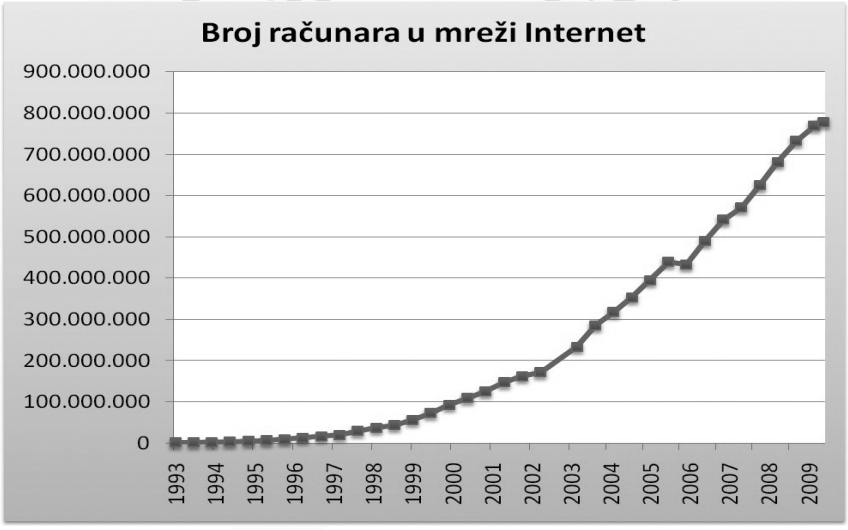
1.3.5. M – trgovina

Mobilno trgovanje ili m-trgovanje se odnosi na upotrebu bežičnih digitalnih uređaja u cilju obavljanja transakcija na Webu. Tipični terminalni uređaji su mobilni telefon ili Palm računari. Nakon uspostave konekcije, mobilni potrošač može da obavi više različitih transakcija, kao što su trgovina akcijama, poređenje cena, bankarske transakcije, rezervacije putovanja, i td.

1.4. RAST InternetA I WWW SERVISA

Nezaustavljive tehnološke snage koje stoje iza e-trgovine su Internet i jedan od najrasprostranjenijih njegovih servisa - World Wide Web (WWW). Bez ove dve tehnologije, e-trgovina kakvu danas znamo bi bila namoguća. Internet je svetska mreža računarskih mreža izgrađena prema zajedničkim standardima zasnovanim na TCP/IP protokolu. Stvoren u kasnim 1960.-im da bi povezao mali broj velikih (mainframe) računara i njihovih korisnika, Internet se od tada razvio u najveću svetsku mrežu, povezujući na stotine miliona računara širom sveta. Internet povezuje preduzeća, obrazovne institucije, vladine agencije i pojedince, i pruža korsinicima usluge kao što su e-pošta (e-mail, elektronska pošta), prenos dokumenata, novinske grupe (newgroups), kupovina, pretraga, instant poruke, muzika, video, vesti i td. [7].

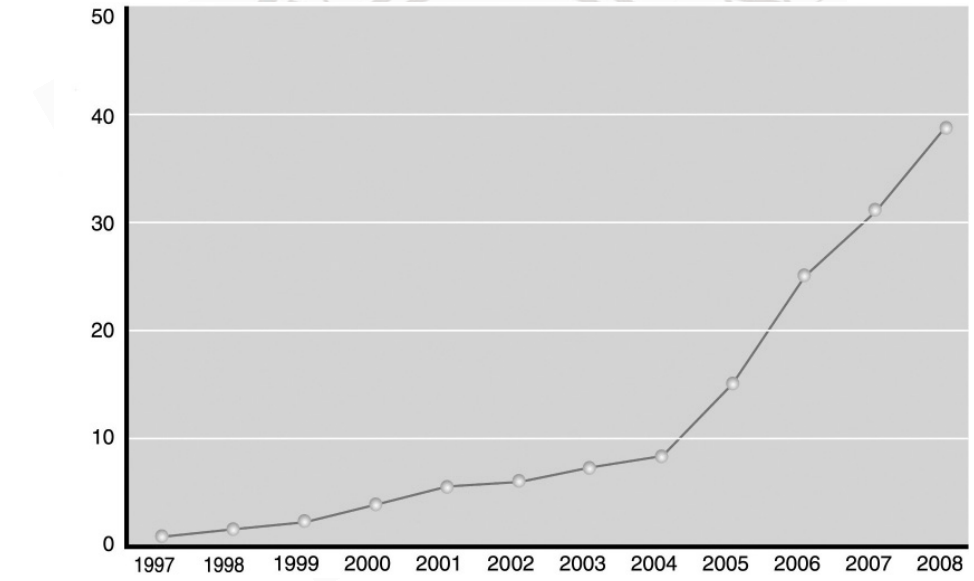
Sl.1.4.1 ilustruje jedan od načina merenja rasta veličine Interneta, gde se uzima u obzir broj host računara (mrežnih servera sa domenskim imenima). U 2000. godini je bilo preko 70 miliona hostova, dok samo deset godina kasnije ovaj broj premašuje 800 miliona, raspoređenih u preko 245 zemalja [8].



Sl. 1.4.1 Rast veličine Interneta, u periodu 1993-2010, meren brojem Internet hostova (servera), koji poseduju imena domena.

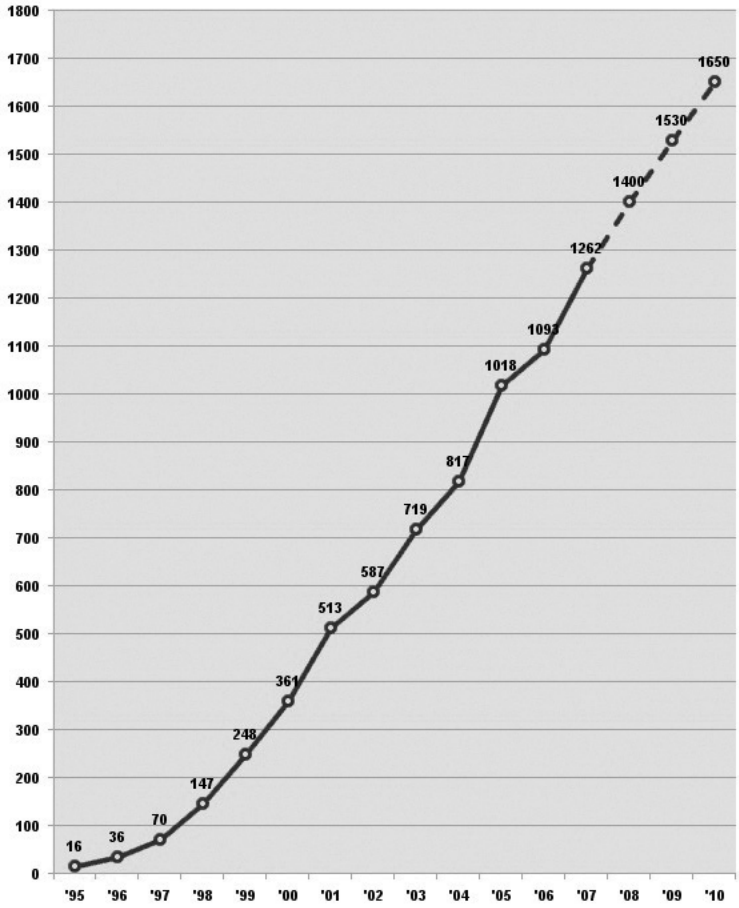
Internet je pokazao izvanredne stope rasta u poređenju sa drugim elektronskim tehnologijama iz prošlosti. Radiju je bilo potrebno 38 godina da dostigne učešće od 30 % u domaćinstvima u Sjedinjenim Državama. Televiziji je bilo potrebno 17 godina da postigne učešće od 30 %. Od pronalaska grafičkog korisničkog interfejsa za World Wide Web u 1993.godini, Internetu je bilo potrebno samo sedam godina da bi postigao učešće od 30 % u domaćinstvima u Sjedinjenim Državama.

World Wide Web je najpoznatiji servis koji funcioniše na infrastrukturi Interneta. Mreža (Web) je aplikacija, koja je učinila Internet trgovinski interesantnim i izuzetno popularnim. Web se razvio početkom 1990.-ih godina i omogućava pristup stotinama milijardi stranica ili multimedijalnih dokumenata kreiranih pomoću programskog jezika HTML (HyperText Markup Language). Ove HTML stranice sadrže multimedijalne informacije – uključujući tekst, grafiku, animacije i druge objekte – koje su dostupne za javnu upotrebu. Na Webu se može pronaći širok spektar informacija, od celokupne zbirke javnih arhiva Komisije za vrednosne papire i razmenu (Securities and Exchange Commission), do kataloga lokalne biblioteke, miliona muzičkih numera i video klipova. Internet pre pojave Weba je prvenstveno korišćen za tekstuelnu komunikaciju, prenos fajlova i daljinsko proračunavanje. Web je uveo multimedijalne mogućnosti, od direktne važnosti za trgovinu. U suštini, Web tehnologija je dodala boju, zvuk i video Internetu, stvarajući komunikacionu infrstrukturu i sisteme za skladištenje informacija koji konkurišu televiziji, radiju, magazinima i bibliotekama. Sadržaj na Internetu se eksponencijalno povećava od 1993. U 2008. bilo je između 35 i 40 milijardi Web stranica, Slika 1.4.2.



Sl. 1.4.2 Rast sadržaja na Webu Internet strane u milijardama, Izvor: Google Inc.

Za sagledavanje potencijalnih mogućnosti e – trgovine od presudne važnosti je dostupnost Interneta na globalnom nivou. Na Sl.1.4.3. dat je prikaz porasta broja korisnika u periodu 1995 – 2010. godina.



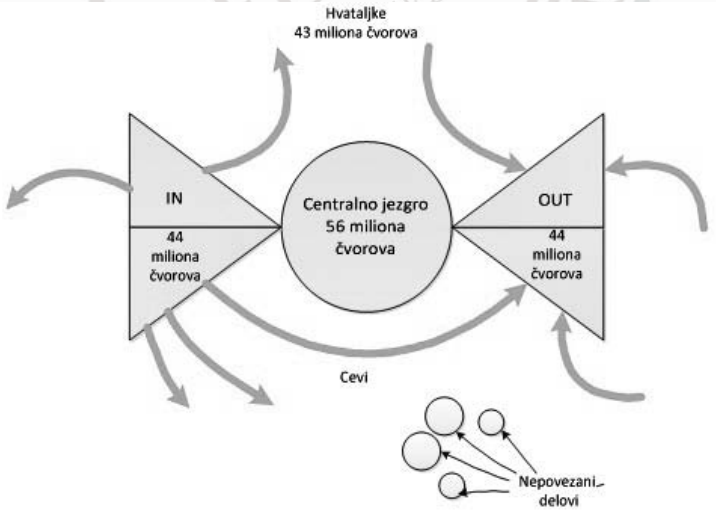
Sl.1.4.3. Rast Internet korisnika na svetskom nivou u periodu 1995 – 2010. U septembru 2010 Internet koristi 1,971 milijardi ljudi, što predstavlja oko 29% od ukupne svetske populacije.

1.5. STRUKTURA POVEZANOSTI WEB-A

Struktura povezanosti Web-a je od posebnog značaja za razumevanje važnih fenomena u okviru e – trgovine. Jasno je da u fizičkom svetu uspeh jedne trgovinske radnje ključno zavisi od njene fizičke pozicioniranosti. Ako je njena lokacija na vrlo posećenim gradskim lokacijama, uspešnost prodaje je gotovo zagarantovana. Šta je ekvivalent u virtuelnom svetu e – trgovine? Nije teško zaključiti da je to stepen vidljivosti sajta virtuelne trgovine sa stanovišta prosečnog korisnika Interneta, koji po pravilu svoju pretragu startuje sa nekog portala snabdevenog dobrim pretraživačem, kao što je Google, Yahoo, Lycos i td.

Web podseća na veliku paukovu mrežu u kojoj se iz bilo koje tačke može doći do bilo koje druge tačke praćenjem odgovarajućih veza – hiperlinkova koji međusobno povezuju pojedine Web stranice. U teoriji malog sveta o mrežama, veruje se da je svaka Web stranica odvojena od bilo koje druge Web stranice sa prosečno 19 "klikova". Teoriju malog sveta su podržavala ranija istraživanja na malim uzorcima Web sajtova. Ali skorašnja istraživanja sprovedena zajednički od naučnika iz IBM, Compaq i AltaVista, pronašla su nešto sasvim drugo. Ovi naučnici su iskoristili mrežni pretraživač "Scooter" za identifikovanje 200 miliona Web stranica i praćenje 1,5 milijardi veza sa ovih stranica.

Istraživanje je otkrilo da Web nije kao paukova mreža, već više kao leptir-mašna, videti Sl.1.5.1. Mreža oblika leptir-mašne ima "čvrsto povezanu komponentu" -centralno jezgro, ili "strongly connected component", SCC, sastavljenu od oko 56 miliona Web stranica. Desno od središta je skup od 44 miliona izlaznih (OUT) stranica, kojima se može pristupiti iz centra, ali koje ne omogućavaju povratak u centar. Izlazne strane su uglavnom korporacijske intranet i ostale mrežne stranice koje su dizajnirane da vas zarobe na sajtu kada mu pristupite. Levo od središta je skup od 44 miliona ulaznih (IN) stranica sa kojih možete doći u centar, ali na koje ne možete doći iz centra. Ovo su skorije stvorene, "novajlijske" - newbie stranice, ka kojima još nije povezana većina centralnih stranica. 43 miliona stranica su razvrstane kao "hvataljke" (tendrils), koje niti vode ka centru, niti im se može pristupiti iz centra. Ipak, stranice hvataljke mogu biti povezane sa ulaznim i izlaznim stranicama. U nekim slučajevima, hvataljke vode jedna ka drugoj bez prolaska kroz centar. Ova vrsta stranica se naziva cevima. Konačno, 16 miliona stranica je potpuno odvojena od svih ostalih stranica.



Sl.1.5.1. Šematska struktura Weba: Izvor: www.searchengineposition.com/Articles/bowtie.html

Slika Weba dobijena ovim istraživanjem se dosta razlikuje od ranijih izveštaja i mišljenja. Trvrđnje da je najveći broj parova mrežnih stranica razdvojen sa velikim bro-

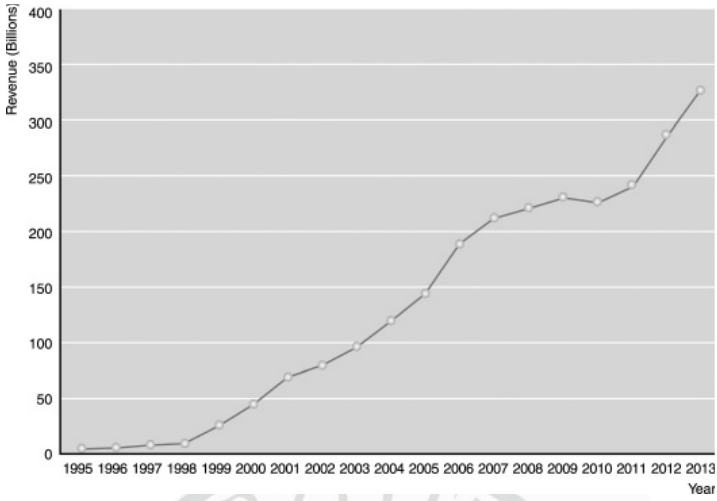
jem veza, skoro uvek ispod 20, kao i da broj veza eksponencijalno raste sa povećanjem Web-a, nisu podržane ovim istraživanjem. U stvari, postoji šansa od 75 % da ne postoji put između jedne nasumice izabrane stanice i neke druge. Sa ovim znanjem postaje jasno zašto najnapredniji pretraživači Weba indeksiraju samo 6 miliona Web sajtova, kada je njihov ukupan broj daleko veći. Većina Web sajtova ne može biti pronađena od pretraživača jer njihove stranice nisu dobro povezane ili spojene sa centralnim jezgrom. Iako prihodi e-trgovine delimično zavise od mogućnosti potrošača da pronađu Web sajtove korišćenjem pretraživača, menadžeri Web sajtova moraju preduzeti posebne postupke da bi obezbedili da njihove stranice budu deo povezanog centralnog jezgra. Jedan od načina da se ovo postigne je da se obezbedi da Web sajt ima što je moguće više veza prema i od ostalih bitnijih sajtova, naročito onih sajtova koji čine centralno jezgro.

1.6. POREKLO I RAST E-TRGOVINE

Teško je precizno odrediti kada je tačno počela e-trgovina. Postoji mnogo oblika koji su prethodili e-trgovini. U kasnim 1970.-im godinama farmaceutska firma Baxter Healthcare je pokrenula uprošćeni oblik B2B e-trgovine koristeći telefonski zasnovane modeme koji su omogućavali bolnicama da naručuju robu od Baxtera. Ovaj sistem je kasnije tokom 1980.-ih proširen u PC zasnovani sistem daljinskih narudžbi i u velikoj meri je kopiran širom Sjedinjenih Država, mnogo pre nego što je Internet postao poslovno okruženje. Standardi Elektronske razmene podataka (Electronic Data Interchange, EDI) su razvijeni u 1980.-im, što je omogućilo firmama da razmenjuju trgovinska dokumenta i obavljaju digitalne transakcije preko privatnih mreža.

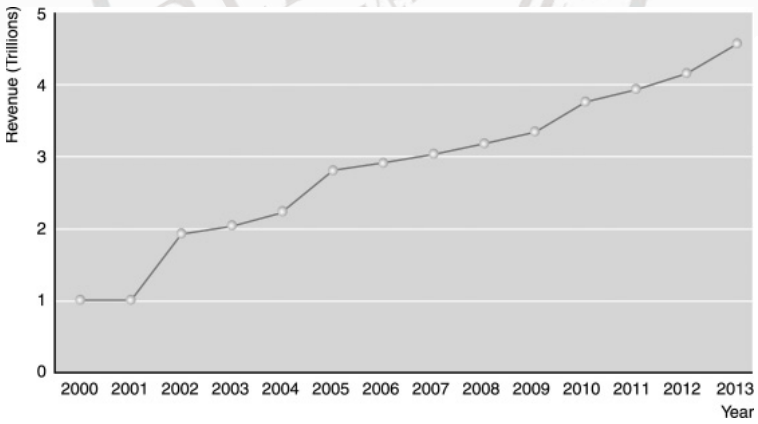
U B2C sektoru, prvi digitalni sistem transakcija velikih razmera je razvijen u Francuskoj u 1981. godini. Francuski Minitel je bio video-tekstualni sistem koji je kombinovao telefon sa 20 centimetarskim (8 inčnim) ekranom. Do sredine 1980.-ih napravljeno je više od 3 miliona Minitela, a danas ih ima oko 15 miliona u upotrebi širom Francuske. Preko 25.000 različitih usluga može biti pronađeno na Minitelu, uključujući agancije za rezervisanje i prodaju karata, turističke usluge, prodaju proizvoda na malo i onlajn bankarstvo. Roba i usluge se plaćaju putem mesečnog telefonskog računa. Ni jedan od takvih sistema koji je prethodio, nije imao funkcionalnost Interneta. Kada danas razmišljamo o e-trgovini, ona je neraskidivo vezana za Internet i počinje 1995. godine, od pojave prvih banera (reklama) postavljenih od ATT, Volvo, Sprint i drugih, na Hotwired.com krajem oktobra 1994. i prvom prodajom banerskog oglasnog prostora od Netscape i Infoseek početkom 1995. godine. Od tada, e-trgovina je najbrže rastući oblik trgovine u Sjedinjenim Državama. Na Sl 1.6.1 i 1.6.2 predstavljen je razvoj B2C e-trgovine i B2B e-trgovine u periodu od 1995. do 2009. godine sa prognozom do 2013. godine.

Oba grafikona prikazuju visoko stopu rasta, ali treba primetiti da dolarski iznosi B2B e-trgovine izrazito nadmašuju one od B2C.



Sl. 1.6.1 Rast B2C e-trgovine Izvor: U.S. Census Bureau, 2009.

U početnim godinama B2C e-trgovina se utrostručavala ili udvostručavala svake godine. Ova eksplozivna stopa rasta je kasnije smanjena. U budućim godinama se očekuje da e-trgovina raste po stopi od 45 % do 55 % godišnje, sa sezonskim vrhuncima koji pokazjuju veće prihode u poređenju na prethodnu godinu. [6]



Sl. 1.6.2 Rast B2B e-trgovine. B2B trgovina je desetostruko veća od B2C trgovine. Izvor: U.S. Census Bureau, 2009.

Iako je e-trgovina u mnogim pogledima nova i različita, bitno je takođe razmatrati i budućnost e-trgovine. Internet i Web su samo dve od mnogih tehnologija koje su značajno promenile trgovinu u Sjedinjenim Državama i širom sveta. Svaka od ovih tehnologija je

stvorila nove poslovne modele i strategije dizajnirane tako da pretvore tehnološke inovacije u poslovne prednosti i profit. Bila je praćena eksplozivnim početnim rastom, za koji je karakteristična pojava hiljada novostvorenih preduzetničkih kompanija, što je naknadno praćeno njihovim smanjenjima, a zatim i dugoročnim uspešnim iskorišćavanjem tehnologija od firmi koje su uspele da se dokažu. U slučaju automobila, na primer, u 1915. je bilo preko 250 proizvođača automobila u Sjedinjenim Državama. Do 1940. bilo ih je pet. U slučaju radija, u 1925. je bilo preko dve hiljade radio stanica širom Sjedinjenih Država, većina je emitovala za obližnja domaćinstvima i bila je vođena od strane amatera. Do 1990. je bilo manje od 500 nezavisnih stanica. Postoji mnogo razloga za verovanje da će e-trgovina pratiti sličan obrazac.

Iako je e-trgovina rasla eksplozivno, nema garancije da će nastaviti da se razvija po ovim stopama i mnogo je razloga za verovanje da će rast e-tgovine dostići vrhunac kada se suoči sa sopstvenim bitnim ograničenjima. Na primer, B2C e-trgovina čini još uvek mali deo (oko 1 %) od ukupnog maloprodajnog tržišta. Sa sadašnjom stopom rasta, ukupna B2C e-trgovina će se približno izjednačiti sa godišnjim prihodom kompanije Wal-Mart – najvećim i najuspešnijim svetskim prodavcem na malo.

1.7. MOGUĆA OGRANIČENJA RASTA B2C E -TRGOVINE

Postoji nekoliko ograničenja B2C e-trgovine koja potencijalno mogu da limitiraju njenu stopu rasta i njenu krajnju veličinu. Tabela 1.7.1 opisuje neka od ovih ograničenja.

OGRANIČENJA RASTA E-TRGOVINE	
OGRANIČAVAJUĆI FAKTOR	KOMENTAR
Domaćinstva	Trenutno 72 % domaćinstava imaju PC
Skupa tehnologija	Korišćenje Interneta zahteva PC od 400 $ (najmanje) i 10 - 60 $ mesečno za troškove priključivanja
Složeni softverski interfejs	Korišćenje mreže zahteva instalaciju složenih operativnih sistema i skupa aplikacija kojima je mnogo teže upravljati nego televizorom ili telefonom
Skup složenih veština	Veštine neophodne za efektivno korišćenje Interneta i e-trgovine su mnogo složenije nego recimo kod televizije ili novina
Neprestana kulturna privlačnost fizičkih tržišta i tradicionalnih iskustava kupovine	Za mnoge, kupovina je kulturni i društveni događaj gde se ljudi direktno sreću sa trgovcima i ostalim potrošačima. Ovo iskustvo se još ne može kopirati u digitalnoj formi
Neprestana globalana nejednakost koja ograničava pristup telefonima i ličnim kompjuterima	Većina stanovništva nema telefonske usluge, PC, ili mobilni telefon

Tabela 1.7.1. Neki faktori ograničenja rasta e-trgovine

Neka od ovih ograničenja mogu biti uklonjena u narednoj deceniji. Na primer, verovatno je da će se cena PC opdati u godinama koje dolaze. Ovaj detalj, udružen sa u poboljšanjima mogućnosti kao što je spajanje sa televizijom, pristup bibliotekama zabavnih filmova zasnovan na plati-pa-gledaj metodi i druga softverska poboljšanja, će verovatno povećati stepen prodora među domaćinstva u SAD, na nivo prodora kablovske televizije (oko 80 %). PC operativni sistemi će se takođe verovatno sa sadašnjih Windows platformi razviti u pravcu mnogo jednostavnijih panela, sličnih interfejsu prisutnom na Palm uređajima veličine dlana.

Najznačajnija tehnologija koja može umanjiti barijere pristupa Internetu je bežična mreža. Trenutno je u upotrebi oko 285 miliona bežičnih telefona u Sjedinjenim Državama, što predstavlja gotovo 91% ukupne populacije. Na svetskom nivou broj korisnika mobilnih telefona iznosi 5 milijardi ili oko 67% ukupne svetske populacije [9].

Neka od ograničenja navedenih u Tabeli 1.7.1 će verovatno opstati. Na primer, veoma je malo verovatno da će se iskustvo digitalne kupovine bilo kad izjednačiti sa društvenim i kulturnim iskustvom koje mnogi očekuju od tradicionalnog okruženja za kupovinu. Dalje, većina svetskog stanovništva neće moći da pristupi Internetu zbog ograničenog pristupa tehnologiji i jezičkih prepreka. Verovatno je da će uticaj tehnoloških ograničenja rasta e-trgovine vremenom opadati, a da će društvena i kulturna ograničenja ostati i dalje značajan faktor u ograničavanju rasta e-trgovine.

1.8 E-TRGOVINA I

Iako je e-trgovina skorašnja pojava iz 1990.-ih, ona već ima svoju istoriju. Istorija e-trgovine može biti podeljena u dva perioda koje nazivamo E-trgovina I i E-trgovina II [10], [11]. E-trgovina I je period eksplozivnog rasta, koji je počeo u 1995. sa prvom širokom upotrebom mreže za reklamiranje proizvoda i završio se u 2000. kada je došlo do sloma vrednosti "tačka.com" (dot.com) kompanija na tržištu akcija. E-trgovina II je počelo u januaru 2001., do kada se odigralo otrežnjujuće preispitivanje e-trgovinskih kompanija i vrednosti njihovih akcija. Svaki od ovih perioda e-trgovine karakteriše skup vizija i pokretačkih faktora.

E-trgovina I je bilo jedno od najeuforičnijih vremena u Američkoj trgovinskoj istoriji. Osnovano je na hiljade dot.com kompanija, podržanih sa preko 125 milijardi $ finansijskog kapitala. To je bio jedan od najvećih izliva ulagačkog kapitala u istoriji Sjedinjenoih Država. Za informatičare, E-trgovina I je period intenzivnog uvođenja u praksu niza informacionih tehnologija koje su razvijane tokom perioda od četrdeset godina, uključujući Internet i PC tehnologiju, lokalne i regionalne računarske mreže. Vizija se odnosila na opšte komunikaciono i računarsko okruženje, kome bi svako mogao da pristupi, koga ne bi kontrolisala ni jedna nacija, već je slobodno za sve. Verovali su da bi Internet i e-trgovina koja je ponikla na ovoj infrastrukturi, trebali da ostanu samo-upravljano i samo-regulisano okruženje.

Za ekonomiste, e-trgovina je povećala šanse za ostvarenje savršenog *Bertrand tržišta* – tržišta gde su cene, troškovi i kvalitetne informacije podjednako dosupne, gde se praktično neograničen skup dobavljača međusobno takmiči i gde potrošači imaju pristup svim bitnim tržišnim informacijama širom sveta. Trgovci bi zauzvrat imali podjednak direktan pristup stotinama miliona potrošača. U ovom približno savršenom informacionom tržišnom prostoru, transakcioni troškovi bi se znatno smanjili, jer troškovi potrage za cenama, opisima proizvoda, nagodbama o plaćanju i troškovi izvršenja narudžbine, bi se dramatično snizili. Novi "kupovni bot" programi (programi za podršku) bi automatski pretraživali celokupni Web radi pronalaženja najbolje cene i vremena isporuke. Za trgovce, troškovi potrage za potrošačima bi takođe opali – umanjujući potrebu za nepotrebnim reklamiranjem. Cene, pa čak i troškovi, bili bi sve više transparentni za potrošača, koji bi sada mogao da zna tačno i trenutno za većinu proizvoda o svetski najnižim troškovima, kvalitetu i dostupnosti. Informaciona asimetrija bi bila značajno smanjena. Uz trenutnu prirodu Internet komunikacija, dostupnost savremenih prodajnih informacionih sistema i niske troškove promene cene na Web sajtu (niski *meni troškovi*, menu costs), proizvođači bi mogli *dinamički određivati cene* svojih proizvoda odražavajući trenutnu tražnju. Zauzvrat, nestali bi tržišni posrednici (dogodila bi se dezintermedijacija, ukidanje posredovanja) – distributeri, prodavci na veliko i drugi tržišni činioci koji posreduju između proizvođača i potrošača, pri čemu svaki od njih zahteva svoj deo prihoda i podiže ukupne troškove. Proizvođači i kreatori sadržaja bi razvili direktne tržišne odnose sa svojim potrošačima. Rezultujuća jaka konkurencija, umanjenje učešća posrednika i niži transakcioni troškovi, eliminisali bi robne marke i zajedno sa tim, mogućnost monopolskih profita zasnovanih na robnim markama, geografiji ili specijalnom pristupu činiocima proizvodnje. Cene proizvoda i usluga bi padale do tačke gde bi cena pokrivala troškove proizvodnje plus poštenu, "tržišnu stopu" zarade na kapital, plus dodatne male isplate za preduzetnički napor, koji ne bi dugo trajao. Bile bi uklonjene nepravedne konkurentske prednosti, kao i visoke zarade na investirani kapital. Ova vizija se zove trgovina bez frikcije, friction-free, bez otpora, trenja, neslaganja.

Tokom I perioda e-trgovine ideja o trgovini bez frikcije je bila nepoznata preduzetnicima, njihovim finansijskim pomagačima i marketinškim profesionalcima. Za njih je e-trgovina je predstavljala mogućnost da profitiraju daleko iznad uobičajenih zarada na investicije, daleko iznad troškova pozajmljivanja kapitala. Trgovinski prostor za e-trgovinu je nudio mogućnost pristupa milionima potrošača širom sveta koji su koristili Internet i mogućnost korišćenja skupa marketinških komunikacionih tehnologija (e-pošta i Web stranice), što je bilo jeftino i efikasno. Ove nove tehnologije su dozvoljavale segmentiranje tržišta na grupe sa različitim potrebama i cenovnom osetljivošću, ciljajući na segmente utvrđenim robnim markama. Rezultat je bio precizno pojedinačno pozicioniranje proizvoda i cena za svaku grupu - segment. U ovom novom tržišnom prostoru, ekstra profit bi odlazio onom ko je prvi povukao potez (first mover) - onim firmama koje se prve pozicioniraju na tržišta u određenoj oblasti i koje se brzo premeštaju radi sticanja svog udela na tržištu. Prvopotezni bi mogli brzo izgaditi baze podataka o potrošačima, rano stvoriti prepoznatljive robne marke, formirati potpuno nove distributivne kanale, a zatim odbi-

jati konkurenciju ugrađivanjem *troškova prelaska* (switching costs) ka njihovim kupcima. Koristeći nove tehnologije, onlajn preduzeća bi mogla razviti on-line zajednice, koje nisu dostupne tradicionalnim trgovcima. Ove potrošačke zajednice bi takođe obezbeđivale dodatnu vrednost i bilo bi ih teško kopirati od tradicionalnih trgovaca. Vlada mišljnje da kada se potrošači jednom naviknu na korišćenje jedistvenog kompanijskog Web interfejsa i niza njegovih odlika, ne mogu se lako prebaciti kod konkurenata.

Mrežni efekat nastaje kada svi učesnici ostvajuju koristi zbog činjenice da svi koriste iste alate ili proizvode, kao što su na primer zajednički operativni sistem, telefonski sistem ili softverska aplikacija, čija vrednost raste time što ih veći broj korisnika prihvata. Preduzetnici tvrde da bi se pokrenuo ovaj proces da je neophodno da cene budu dovoljno niske da bi privukle potrošače i odbile konkurenciju. E-trgovina je ipak potpuno novi način kupovine, koji bi trebao da pruži potrošačima neke koristi u vezi troškova posredovanja. Pretpostavlja se da je poslovanje na Webu mnogo efikasnije u poređenju sa tradicionalnim "cigla i malter" preduzećima i čak i u poređenju sa direktnim poštanskim kataloškim poslovanjem, jer su troškovi sticanja i zadržavanja potrošača su znatno niži. Sa ovakvom dinamikom, u početnim fazama učešća na on line tržištu, broj posetilaca na sajtu i prihodi postaju mnogo bitniji, nego zarada ili profiti. Preduzetnici i njihovi finansijski pomagači su očekivali u I dobu e-trgovine da bi profitabilnost nastupila tek posle nekoliko godina gubitaka.

I period e-trgovine je vođen uglavnom vizijama o profitiranju na osnovu novih tehnologija, sa naglaskom na brzo postizanje velike tržišne uočljivosti. Izvor finansiranja su bili venture kapitalni fondovi. Ideologija perioda naglašava neregulisani "divlje zapadni" karakter Weba, osećanje da vlade i sudovi ne bi mogli ograničiti ili regulisati Internet, da su tradicionalne korporacije isuviše spore i zarobljene u starom načinu obavljanja poslova, da bi mogle da postanu konkurentne e-trgovini. Mladi preduzetnici su prema tome bili pogonska sila rizičnih ulaganja e-trgovine I, podržana velikim iznosima novca investiranim od venture kapitalista. Naglasak je bio na razgrađivanju tradicionalnih distribucionih kanala i dezintermedijaciji postojećih kanala, korišćenjem novih čistih onlajn kompanija. Na ukupnom nivou, e-trgovina I se odlikuje eksperimentisanjem, kapitalizacijom i hiperkonkurencijom .

1.9 E-TRGOVINA II

Slom vrednosti tržišta akcija kompanija e-trgovine I u 2000. godini je događaj kojim se označava kraj ovog perioda. Bilo je dosta razloga za taj slom. Deo uspona tehnoloških akcija, naročito onih kojima je trgovano na NASDAQ tržištu, bio je očekivan, zbog ogromnih kapitalnih troškova za informacione tehnologije u velikim američkim firmama, koje su dograđivale svoje interne informacione sisteme da bi odolele izazovima 2000. godine (Y2K). Verovalo se da je prost prelaz sa 1999. na 2000. predstavljao značajnu pretnju

korporacijskim sistemima. Kada su ovi sistemi nadograđeni, kapitalni troškovi informacione tehnologije su opali, obarajući prognoze o zaradama tehnoloških kompanija.

Drugo, početkom 2000. je postalo jasno da je telekomunikaciona industrija izgradila suvišne kapaciteta za brze telekomunikacione mreže zasnovane na optičkim vlaknima, što je dovelo do pada zarada u ovom sektoru, uz bankrotstva mnogih manjih firmi nesposobnih da servisiraju dugove nastale tokom izgradnje mreža velikih brzina. Procenjeno je da 250 milijardi $ dugova u telekomunikacionom sektoru neće biti otplaćeni.

Treće, Božićna sezona e-trgovine u 1999. je obezbedila manji porast prodaje nego što je procenjivano i još bitnije, pokazala je da e-trgovina nije lak posao. Mnogi dot.com trgovci na malo – kao što je eToys.com – nisu mogli da isporučuju u blagovremenim rokovima. Ovo je generalno poljuljalo poverenje u B2C e-trgovinu.

Četvrto, i možda najvažnije, vrednovanja dot.com i tehnoloških kompanija su porasla tako visoko da su čak i oni koji su pružali pordšku postavljali pitanje da li bi zarade ovih kompanija mogle da rastu dovoljno brzo da bi opravdale cene akcija. Neke visoko tehnološke kompanije su imale vrednost akcija 400 puta veći u odnosu na nivo prema njihovim zaradama, dok su se akcije tradicionalnih firmi prodavale za 10 do 15 puta više u odnosu na njihove zarade. Kako se ispostavilo, većina dot.com kompanija – onih specifično posvećenih e-trgovini – u stvari nije imale nikakvu zaradu. Većina je u stvari gubila novac prikazujući rast prihoda.

Slom tržišta akcija dot.com kompanija je vodio otrežnjavajućem preispitivanju budućnosti e-trgovine i metoda za postizanje tržišnog uspeha. E-trgovina II – drugi period u evoluciji e-trgovine – počeo je u januaru 2001.

Dok II period e-trgovine zadržava ekstremno brz tempo rasta broja potrošača i visine prihoda, jasno je da mnoge vizije e-trgovine razvijene tokom E-trgovine I nisu ostvarene. Na primer, vizije ekonomista o trgovini bez frikcije još nisu potpuno ostvarene. Cene nekad jesu niže na Web-u, ali su niske cene pre svega funkcija preduzetničke prodaje proizvoda ispod njihovih troškova. Potrošači su manje cenovno osetljivi nego što je očekivano; iznenađujuće ja da Web sajtovi sa najvećim prihodima takođe imaju i najveće cene. Opstaje značajna disperzija cena na mreži, a koncept jednog sveta, jednog tržišta i jedne cene je oslabio kako su preduzetnici otkrivali nove načine za diferencijaciju njihovih proizvoda i usluga. Na primer, cene knjiga i CD-ova se razlikuju za čak i do 50 %, cene avionskih karata za čak i do 20 %. Robne marke ostaju i dalje bitne za e-trgovinu – potrošači veruju nekim firmama više nego ostalim da će na vreme biti isporučen visoko kvalitetan proizvod. Bertrand-ov model ekstremne tržišne efikasnosti se još nije ostvario. Trgovci i marketari neprekidno uvode informacione asimetrije. Troškovi pretrage su možda sniženi na ukupnom nivou, ali ukupni trošak transakcije pri stvarnom obavljanju transakcije u e-trgovini ostaje veoma visok, jer korisnici donose veliki broj novih odluka: Da li će trgovac zaista isporučiti? Koji je vremenski okvir za isporuku? Da li trgovac zaista ima artikal među zalihama?. Oko 65 % e-trgovinskih kupovina su prekinute u fazi korpe za kupovinu, zbog ovakvih potrošačkih dilema. U oblastima mnogih proizvoda je lakše telefonirati proverenom kataloškom trgovcu, nego naručiti na Web sajtu. Konačno, po-

srednici nisu nestali kao što je predviđano i veoma malo prerađivača ili proizvođača je zaista razvilo jedan-na-jedan prodajni odnos sa svojim krajnjim potrošačima. E-trgovina je stvorila mnoge nove mogućnosti za preprodavce u vidu prikupljanja sadržaja, proizvoda i usluga u okviru Web portala i time im omogućila da se predstave kao "novi" posrednici. Yahoo.com i Amazon.com su dva primera ove vrste novih posrednika.

Prednosti prvopoteznih su se ostvarile samo kod veoma male grupe Web sajtova. Istorija nas uči da su se često prvopotezni pokazali gubitnicima na dugi rok. Njih na tržištu često zamenjuju „brzo prateće" firme, sa značajnim finansijskim, marketinškim, pravnim i proizvodnim sredstvima, neophodnim za razvoj zrelih tržišta, što se potvrdilo i u slučaju e-trgovine. Jedan broj e-trgovinkih prvopoteznih kompanija, kao eToys.com, FogDog.com (sportska roba), Furniture.com, i Eve.com (kozmetički proizvodi), izgubili su tržišnu igru. Troškovi sticanja i zadržavanja potrošača su se pokazali veoma visokim, tako da neke firme plaćaju i do 400 $ za sticanje pojedinačnog novog potrošača, kao što je to slučaj kod E-Trade.com i drugih firmi za finansijske usluge. Ukupni troškovi poslovanja na Web-u – uključujući troškove tehnologije, dizajna i održavanja sajta i troškovi neophodnih skladišta – nisu niži od troškova sa kojima se suočavaju najefikasnije prodavnice od cigala i maltera. U Tabeli 1.9.1 data su komparativna poređenja nekih bitnih karakteristika e-trgovine I i II.

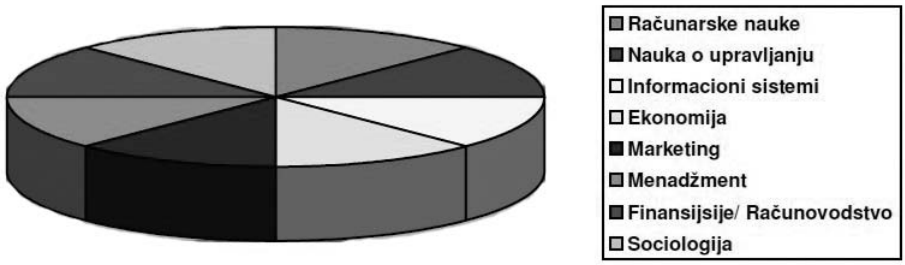
POREĐENJE E-TRGOVINE I i E-TRGOVINE II	
E-TRGOVINA I	E-TRGOVINA II
Tehnološki vođena	Poslovno vođena
Naglasak na rastu prihoda	Naglasak na zaradi i profitu
Finasiranje venture kapitalom	Tradicionalno finansiranje
Neregulisana	Snažnija regulacija i upravljanje
Preduzetnička	Velike tradicionalne firme
Dezintermedijacija	Jačanje posrednika
Savršena tržišta	Nesavršena tržišta, robne marke i mrežni efekti
Čiste onlajn strategije	Mešovite "klikovi i cigle" strategije
Prednosti prvopteznih	Snaga strateških pratilaca

Tabela 1.9.1 Sumarni prikaz poređenja nekih bitnih karakteristika e-trgovine I i II.

1.10 NAUČNE DISCIPLINE KOJE SE BAVE E-TRGOVINOM

Fenomen e-trgovine je u toj meri širok da je neophodan multi-disciplinarni pristup u istinskom sagledavanju svih njenih fenomena. Dovoljan dokaz o složenosti i važnosti ove discipline je njen prodor u akademske sfere. Gotovo da ne postoji savremeni univeryitet u

svetu koji danas u svoje kurikulume ne uključuje i predmet e-trgovina u celini ili u nekom od njenih aspekata. Na Sl.1.10.1 dat je pregled disciplina koje su direktno uključene u proučavanje i razumevanje e-trgovine. Postoje dva dominantna pristupa u razumevanju e-trgovine: tehnički i bihevioristički.



Sl 1.10.1. Discipline koje se bave e-trgovinom

1.10.1.Tehnički pristup

U okviru ovog pristupa naučnici koji se bave računarskim naukama su zainteresovani za e-trgovinu kao primer primene Internet tehnologije. Oni se bave razvojem računarskog hardvera, softvera, telekomunikacionih sistema i sistema zaštite informacionih tokova. Naučnici koji se bave menadžmentom su prvenstveno zainteresovani za izradu matematičkih modela poslovnih procesa i njihovu optimizaciju. Proučavanje e-trgovina za njih predstavlja priliku da saznaju kako kompanije mogu koristiti Internet da bi ostvarile efikasniju poslovnu operativnost.

1.10.2. Biheviorstički pristup

U behiviorističkom pristupu, istraživači informacionih sistema su prvenstveno zainteresovani za e-trgovinu zbog njenih posledica na lanac vrednosti pojedinih kompanija i industrije u celini, industrijsku strukturu i korporacijsku strategiju. Oblast informacionih sistema obuhvata tehničke i biheviorističke pristupe. Na primer, tehničke grupe unutar specijalnosti informacionih sistema se koncentrišu na sisteme za efikasnu potragu za informacijama, dizajn alata za pretraživanje informacionih sadržaja i veštačku inteligenciju. Ekonomisti se koncentrišu na ponašanje potrošača na Web sajtovima i na svojstva digitalnih elektronskih tržišta. Kroz obe ove oblasti, ekonomisti dele interesovanje sa poznavaocima marketinga, koji se fokusiraju na e-trgovinski odgovor potrošača na marketinške i reklamne kampanje i mogućnosti firmi da stvaraju robne marke, segmentiraju tržište, ciljaju na određenu publiku i pozicioniraju svoje proizvode. Poznavaoci menadžmenta se fokusiraju na preduzetničko ponašanje i izazove sa kojima se suočavaju mlade firme koje treba da razviju organizacione strukture u kratkim vremenskim okvirima. Poznavaoci finansija

i računovodstva usredsređuju se na vrednovanje e-trgovinskih firmi i računovodstvene postupke. Sociolozi, i u manjoj meri psiholozi, se usredsređuju na proučavanje ukupnog stanovništva u vezi korišćenja Interneta, ulozi socijalne nejednakosti i korišćenju mreže kao ličnog i grupnog komunikacionog alata. Poznavaoci prava se interesuju za pitanja kao što su očuvanje prava intelektualne svojine i privatnosti. Ni jedan ugao posmatranja ne treba da dominira istraživanjem e-trgovine. Pravi je izazov naučiti dovoljno o različitim naučnim disciplinama u cilju shvatanja značaja e-trgovine u svoj svojoj potpunosti.

1.11 LITERATURA

[1] http://www.amazon.com/

[2] http://www.budde.com.au/Research/2009-Global-Digital-Economy-E-Commerce-M-Commerce-Trends-Statistics.html?r=51

[3] K.Laudon, C. Traver, *E-Commerce: Business, Technology Society,* 5.th ed., Boston, Addison-Wesley, 2009.

[4] http://www.Internetworldstats.com/stats.htm

[5] http://europe.wsj.com/home-page

[6] http://www.emarketer.com/

[7] M.Milosavljević, G. Grubor, M. Veinović, *"Informatika"*, Univerzitet Singidunum, 2009.

[8] http://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_hosts

[9] http://en.wikipedia.org/wiki/List_of_countries_by_number_of_mobile_phones_in_use

[10] E.Turban, D.King, D. Viehland, J.Lee, *Electronic Commerce 2006, A Managerial Perspective*, Pearson Prentice Hall, 2006.

[11] M.Fasil, "*Agent Technology for e-Commerce*", John Wiley & Sons, 2007.

2. ELEKTRONSKI MODELI I KONCEPTI U ELEKTRONSKOJ TRGOVINI

2.1 UVOD

U toku dosadašnjeg razvoja elektronske trgovine, mnoge dot.com kompanije su napravile izvanredne uspehe i podstakle razvoj čitavih segmenata tržišta, proizvoda i usluga. S druge strane, još je veći broj kompanija koje su izneverile očekivanja svojih investitora i nakon početnih uspeha doživele naoko neočekivani neuspeh. Da li je moguće unapred, pre izlaska na tržišnu arenu, imati dovoljno čvrstih argumenata za uspešno poslovanje? Da li se unapred sa dovoljnom verovatnoćom može tvrditi da je planirani poslovni poduhvat nerealan i da je teško očekivati brz povraćaj uloženog kapitala? Pažljiva analiza pokazuje da je u većini slučajeva neuspešnog poslovanja, poslovni model kompanije bio pogrešan od samog početka, i obrnuto, da je biznis model uspešnih kompanija iskoristio jedinstvene prednosti Interneta i WWW servisa obezbeđujući kupcima vredne proizvode i usluge, zasnovane na efikasnim poslovnim procesima, dajući na kraju profitabilni poslovni rezultat. Osim toga, uspešni biznis modeli su po pravilu posedovali važno svojstvo skalabilnosti, koje se sastoji u održavanju efikasnosti i profitabilnosti poslovanja sa porastom obima poslovanja.

Šta je biznis model i zašto je od ključne važnosti u celokupnom poduhvatu startovanja, održavanja i rasta jedne dot.com kompanije upoznaćemo se u ovom poglavlju. Nakon izlaganja najvažnijih komponenti biznis modela, sledi prikaz osnovnih biznis modela u B2C i B2B elektronskom poslovanju, kao i biznis modela elektronskog poslovanja u nastajanju, kao što su C2C, P2P i mobilno elektronsko poslovanje. Poglavlje se završava analizom promena koje su nastale u poslovnom okruženje u poslednjih petnaestak godina pod uticajem Interneta i elektronske trgovine.

2.2. POSLOVNI MODELI ELEKTRONSKE TRGOVINE

Napomenimo na samom početku da ćemo pođednako koristiti izraze poslovni i biznis model imajući u vidu isti pojam. Kao i u većini termina preuzetih iz engleskog jezika oslanjanje samo na odgovarajući prevod na srpski jezik rizikuje šire razumevanje. Poslovni (biznis) model je skup planiranih aktivnosti, odnosno poslovnih procesa, kreiranih u cilju ostvarivanja profita na tržištu. Predstavlja centralni deo biznis plana, pod kojim se podrazumeva dokument u kome se opisuje biznis model. Biznis model elektronske trgovine koristi jedinstvene prednosti Interneta i WWW servisa u cilju sprovođenja planskih aktivnosti za ostvarivanje što bolje pozicije na globalnom otvorenom tržištu elektronske trgovine. U Tabeli 2.1. dat je pregled osam ključnih komponenti biznis modela bez obzira o kojoj vrsti poslovanja se radi. Ove komponente su predlog vrednosti, model prihoda, tržište, konkurencija, konkutrentska prednost, marketinška strategija, organizacioni razvoj i menadžerski tim [1].

KLJUČNE KOMPONENTE BIZNIS MODELA	
Kopmponente	**Ključna pitanja**
Ponuda vrednosti	Zašto bi kupci kupovali kod vas?
Model prihoda	Kako ćete zaraditi novac?
Očekivano tržište	Na koje tržište računate i koliko je ono veliko?
Konkuretsko okruženje	Ko se još nalazi na tržištu koje nameravate da zauzmete?
Konkurentska prednost	Koju posebnu prednost će vaša kompanija doneti na tržište?
Marketinška strategija	Na koji način ćete vršiti promociju vaših proizvoda ili servisa u cilju privlačenja kupaca?
Organizacioni razvoj	Koji oblik organizacione strukture vaše kompanije je neophodan u cilju realizacije biznis plana?
Upravljački tim	Koje vrste znanja i iskustva je potrebno da ima upravljački tim?

Tabela 2.1. Ključne komponente biznis modela

Mnogi autori smatraju da su ponuda vrednosti i model prihoda dve najvažnije komponente biznis modela, mada se pokazuje da su i ostale komponente jednake važnosti u proceni zašto je jedna kompanija bila uspešna ili je doživela neuspeh.

2.2.1 Ponuda vrednosti

Ponuda vrednosti zauzima centralno mesto u biznis modelu. Ovom komponentom biznis modela se definiše na koji način će proizvodi ili usluge kompanije zadovoljiti potrebe kupaca. U cilju razvoja, odnosno analize ponude vrednosti, neophodno je odgovoriti na pitanje zašto će kupci poslovati sa vašom a ne nekom drugom kompanijom? Šta to nudi vaša komanija, što druge kompanije ne nude ili ne mogu da ponude? Sa stanovišta kupca, ponuda vrednosti obuhvata personalizaciju i kastomizaciju ponuđenih proizvoda i usluga, smanjivanje troškova pronalaženja proizvoda i njihove cene, kao i olakšavanje obavljanja celokupne transakcije efikasnim upravljanjem dostavom proizvoda do kupca. Na primer, pre pojave Amazon.com kupci su morali lično da putuju do prodavnice knjiga da bi kupili željeni naslov. U mnogim slučajevima, željena knjiga se nije nalazila u datoj prodavnici i bilo je potrebno više dana ili nedelja da se knjiga dopremi i da kupac ponovo dođe da bi je kupio. Amazon.com je omogućio kupcima kupovinu bilo koje knjige od kuće ili radnog mesta u toku 24 sata svakodnevno, pri čemu je kupac odmah informisan da li je tražena knjiga dostupna ili ne. Ponuda vrednosti Amazon.com je praktično neograničen asortiman i pogodnost kupovine. Po pravilu, kompanije razvijaju svoju ponuda vrednosti na osnovu opšteg stanja na tržištu i trendova u zahtevima kupaca za određenim proizvodima ili servisima.

2.2.2 Model prihoda

Model prihoda u okviru biznis plana opisuje načine na koje će kompanija ostvarivati prihode, generisati dobit i superioran pvraćaj uloženog kapitala. Često se ova komponenta naziva i finansijski model. Da bi smo jednu kompaniju smatrali uspešnom poslovnom organizacijom, nije dovoljno samo da ostvaruje profit, već je potrebno da ostvaruje prihode veće od odgovarjućih alternativnih investicija. Kompanije koje ne prolaze ovaj test, po pravilu nestaju sa tržišta. Iako su do sada razvijeni veoma različiti modeli prihoda, većina kompanija se oslanja na jedan ili neku kombinaciju sledećih osnovnih modela: model reklamiranja, model pretplata, model transakcionih provizija, model prodaje i afilacioni (partnerski) model.

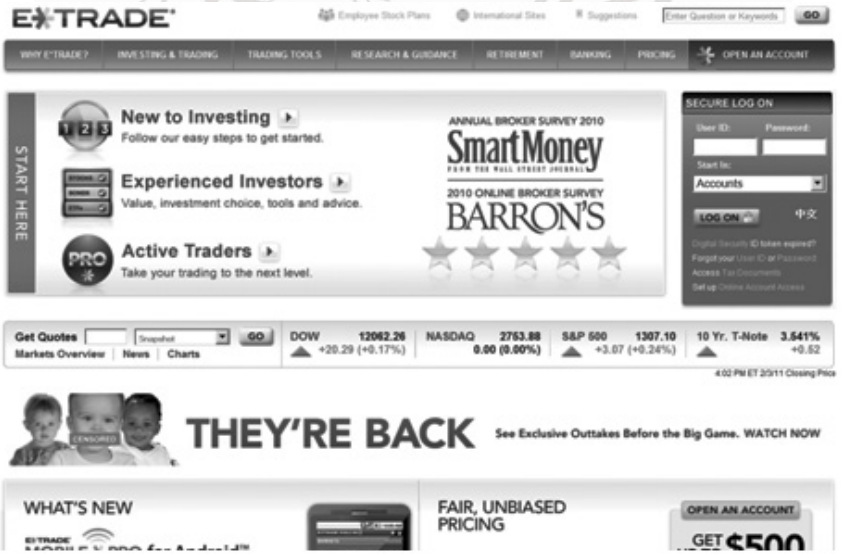
U modelu reklamiranja Web sajt elektronske trgovine, koji svojim posetiocima pruža mogućnost kupovine proizvoda, usluga ili sadržaja, istovremeno obezbeđuje reklamni prostor drugim komapnijama i za tu uslugu dobija odgovarajuće provizije. Oni Web sajtovi koji su u stanju da privuku i zadrže veliki broj posetilaca, ili čiji su posetioci visoko specijalizovani i diferencirani u odnosu na generalnu populaciju, u poziciji su da svoje usluge reklamiranja naplaćuju po višim cenama. Npr. Yahoo.com ostvaruje značajan deo svojih prihoda prodajom prostora za reklamne banere na Web stranicama svojih sajtova. Ovaj model je i dalje primarni izvor prihoda Web baziranog poslovanja.

U model prihoda od pretplata Web sajt koji nudi sadržaje ili servise svojim korisnicima, naplaćuje pretplatu koja omogućava pristup nekim ili svim ovim sadržajima ili servisima. Pretplate su po pravilu mesečne, polugodišnje ili godišnje. Iskustvo pokazuje da generalni korisnici Interneta ne vole pretplate. Odavde sledi da model prihoda zasnovan na ovom mehanizmu može biti uspešan samo ako se sadržaj koji se nudi doživljava kao nosilac izuzetne dodatne vrednosti, kao premijum koji se ne može naći lako na nekom drugom mestu ili zameniti nečim drugim. Npr. Yahoo.com nudi mesečnu pretplatu po ceni $9.95 za tzv. Yahoo Platinum, koja omogućava pristup CNN, NASCAR trkama, ABC vestima i nekim drugim video sadržajima.

U modelu transakcionih provizija kompanija dobija proviziju na osnovu omogućavanja ili izvršenja transakcija. Npr. eBay.com formira onlajn aukcijsko tržište i na osnovu toga dobija provizije od prodavca koji je na osnovu toga ostvario prodaju. E-Trade.com je onlajn broker berzanskih akcija koji dobija provizije na osnovu svake berzanske transakcije obavljene u ime nekog kupca, Sl.2.2.1.

Model prodaje obezbeđuje kompaniji prihode na osnovu prodaje kupcima roba, informacija ili servisa. Amazon.com je primer kompanije koja između ostalih ima i ovaj model prihoda.

Web sajtovi koji imaju afilacioni model prihoda, dobijaju proviziju ukoliko kupci upućeni sa tog sajta na partnerski sajt, obave bilo koju poslovnu transakciju. Na primer MyPoints.com ostvaruje prihode tako što usmeravaju potencijalne kupce ka odgovarajućim kompanijama. Ako kupci prihvate ponudu i izvrše kupovinu, dobijaju odgovarajući broj poena, koje zatim mogu da upotrebe za naredne kupovine, a MyPoints.com dobija odgovarajuću proviziju.



Sl.2.2.1 Prva stranica Web sajta E-Trade.com čiji je model prihoda zasnovan na transakcionim provizijama.

2.2.3 Očekivano tržište

Očekivano tržište se odnosi na tržište na koje se računa, kao i na ukupne potencijalne finansijske resurse ostvarljive na tom tržištu. Očekivano tržište se deli na manje tržišne niše. Realno očekivano tržište se definiše na osnovu potencijalnih prihoda u svakoj od tržišnih niša na kojoj kompanija ima nameru da konkuriše.

2.2.4 Konkurentsko okruženje

Konkurentsko okruženje se odnosi na kompanije koje prodaju slične proizvode i posluju na istom tržištu. Ono obuhvata i prisustvo substitucionih proizvoda, kao i potencijalno novih igrača na tržištu. Određeno je sa više različitih faktora, kao što su broj i veličina aktivne konkurencije, udeo konkurencije u ukupnom zajedničkom tržištu, koliko je konkurencija profitabilna i kolike su cene njihovih proizvoda. Konkurencija može biti direktna i indirektna. Direktni konkurenti su kompanije koje prodaju slične proizvode i usluge na istom segmentu tržišta. Na primer Travelocity.com i Priceline.com su direktni konkurenti pošto obe kompanije prodaju identičan proizvod – jeftine avionske karte. Indirektni konkurenti su kompanije koje mogu biti čak i u različitim industrijskim granama, ali njihovi proizvodi mogu biti zamena jedni drugima. Na primer proizvođači automobila i avionske kompanije posluju u različitim industrijama, ali i dalje su međusobno indirektni konkurenti budući da kupcima nude alternativna transportna sredstva.

Postojanje velikog broja kompanija u nekom tržišnom segmentu može biti znak da je tržište zasićeno i da je na njemu teško ostvariti profit. S druge strane, nedostatak konkurencije može biti ili znak nepopunjenog segmenta tržišta koga treba što pre osvojiti ili pak posledica neuspeha prethodnih pokušaja da se na tom segmetu ostvari profit.

2.2.5 Konkurentska prednost

Jedna kompanija postiže konkurentsku prednost ako uspe da proizvede superiorni proizvod i/ili iznese proizvod na tržište po nižoj ceni od većine ili svih konkurenata [2]. Kompanije se takmiče i u pogledu obuhvata tržišta, koje u tom pogledu može biti lokalno ili globalno. Kompanije koje su u stanju da ponude superiorne proizvode po najnižoj ceni na globalnom tržištu su u najvećoj prednosti. Konkurentska prednost se ostvaruje tako što kompanije na neki način ostvaruju diferencijalni pristup faktorima proizvodnje, za razliku od konkurentskih kompanija kojima to ne polazi za rukom. Na primer, takve kompanije su možda dobile posebno povoljne uslove od dobavljača, prevoznika ili su imale pristup jeftinoj radnoj snazi. U istoj meri to mogu biti faktori sasvim druge prirode, kao što su veće iskustvo i znanje ili lojalnija radna snaga. Konkurentska prednost se može ostvariti i na osnovu posedovanja patentnih prava od značaja za datu delatnost ili povoljniji pristup

finansijskom kapitalu na osnovu mreže bivših poslovnih kolega i partnera. Kaže se da postoji asimetrija ako makar jedan učesnik na tržištu ima više resursa, kao što su znanje, iskustvo, informacije, kapital i td. od ostalih učesnika. Asimetrija omogućava prednost u odnosu na druge, što vodi ka bržem iznošenju na tržište boljih proizvoda po nižoj ceni.

Posebno je značajno istaći jedan poseban izvor konkurentske prednosti: prednost prvog poteza. Stiče je kompanija koja prva iznosi na tržište jedan proizvod ili servis. Ukoliko se nakon prvog poteza na tržištu razvijaju lojalni sledbenici, ili se novi proizvod teško kopira, kompanije prvog poteza mogu dugo vremena zadržati konkurentsku prednost. Takav primer je Amazon.com. Međutim, ukoliko kompanija prvog poteza ne poseduje tzv. komplementarne resurse, kao što su marketing, menadžment, finansijska sredstva ili reputacija, neophodne za održavanje konkurentske prednosti, po pravilu kompanije koje su neposredni konkurenti mogu požnjeti veći deo njihovog početnog uspeha. Arena elektronske trgovine je prepuna uspešnih priča kompanija koje možemo svrstati u tzv. spore pratioce. One duguju svoj uspeh znanju stečenom na neuspehu pionirskih kompanija prvog poteza, na osnovu koga su razvile svoj biznis model i kasnije uspešno ušle na tržište.

Pod nefer konkurentskom prednošću smatraćemo onu nastalu na osnovu faktora koje ostale kompanije ne mogu da priušte. Npr. ime brenda se ne može kupiti i u tom pogledu predstavlja jedan vid nefer prednosti. Kao što ćemo kasnije videti, brendovi se grade oko lojalnosti, poverenja, pouzdanosti i kvaliteta. Kada se jednom dobije, teško se kopira i imitira, a kompanijama koje poseduju brend daje mogućnost da prodaju brendirane proizvode po višim cenama.

Važan pojam u kontekstu tržišnih odnosa i konkurentnosti predstavlja pojam perfektnog tržišta. Na perfektnom tržištu nema konkurentske prednosti ili asimetrije, budući da sve kompanije imaju pođednak pristup svim faktorima produkcije, uključujući i relevantne informacije i znanje. Realno tržište nije perfektno i asimetrije dovode do konkurentske prednosti, u najmanju ruku na kraćim rokovima. Većina konkurentskih prednosti su kratkotrajne, mada ima primera, kao što je Coca – Cola, da ove prednosti mogu trajati decenijama.

2.2.6 Marketinška strategija

Bez obzira kakav je kvalitet neke kompanije, poslovni poduhvat će propasti ukoliko se ne izvrši odgovarajući marketing, odnosno proizvodi kompanije ne učine adekvatno dostupnim potencijalnim kupcima. Pod marketingom se podrazumevaju sve aktivnosti kojima se ostvaruje promocija proizvoda i usluga potencijalnim korisnicima. Marketinška strategija je plan koji razrađuje načine na koji će kompanija ući na novo tržište i privući nove kupce.

2.2.7 Organizacioni razvoj

Iako je čest slučaj da jedan poslovni poduhvat započinje idejama i vizijama jednog čoveka, praktično je nemoguće da pojedinac sam razvije celokupan poslovni sistem većeg obima poslovanja. U većini slučajeva kompanije koje se brzo razvijaju, kao što je slučaj u oblasti e-trgovine, zahtevaju odgovarajući broj zaposlenih i razvijene poslovne procedure, što nameće potrebu za organizacijom koja će efikasno implementirati biznis planove i strategije.

Nedostatak organizacione strukture i pratećih kulturoloških vrednosti je čest uzrok neuspeha mnogih kompanija iz domena e-trgovine. Osim toga, budući da se ove kompanije po pravilu brzo razvijaju, neophodan je plan organizacionog razvoja koji opisuje na koji način će kompanija organizovati izvršenje neophodnih poslova iz delokruga svoje delatnosti. Tipična je podela poslova na funkcionalne departmane, kao što su proizvodnja, dostava, marketing, podrška kupaca i finansije. Zatim se definišu poslovi u okviru svake funkcionalne celine, nakon čega se popunjavaju odgovarajućim kadrom.

Na samom početku razvoja jedne kompanije, logično je objedinjavanje pojedinih funkcionalnosti i prijem kadrova koji su šire osposobljeni za veći broj poslova. Sa potonjim razvojem i rastom obima poslovanja, kadrovi postaju sve specijalizovaniji. Tako na primer u početku razvoja jedan čovek može biti dovoljan za sve poslove vezane za marketing, da bi se nakon uspešnog razvoja kompanije ovo radno mesto podelilo na nekoliko specifičnih zadataka i radnih mesta u okviru sprovođenja marketinške strategije kompanije.

2.2.8 Upravljački tim

Neosporno je da upravljački tim predstavlja najvažniji element biznis plana, budući da je on odgovoran za rad ceolkupnog modela. Jak upravljački tim obezbeđuje iskustvo i specifična znanja za uspešno vođenje kompanije i istovremeno šalje jaku poruku spoljašnjim investitorima u pogledu ozbiljnosti kompanije i njenih poslovnih potencijala i perspektiva. Osim toga, jak upravljački tim može bolje da prepozna eventualne slabosti biznis modela i na vreme predlože njegove izmene. Izazov u nalaženju dobrog upravljačkog tima leži u činjenici da je bitno pronaći ne samo iskusne menadžere, već i menadžere koji na osnovu prethodnih iskustava poseduju sposobnost primene ovih znanja na nove situacije. Dobro uputstvo za kompletiranje upravljačkog tima je analitičko razmatranje pojedinih sposobnosti koje moraju posedovati, kao što su npr. tehnička potkovanost, vrsta radnog iskustva, staž proveden na pojedinim upravljačkim funkcijama itd.

2.3 OSNOVNI B2C POSLOVNI MODELI

Poslovni modeli se mogu kategorisati na različite načine, a mi smo se opredelili za kategorizaciju shodno pripadajućem sektoru elektronske trgovine, dakle B2C, C2C, B2B biznis model i td. Shodno tome, dva vrlo slična biznis modela mogu pripadati u više nego jednom sektoru. Npr. biznis model onlajn prodaje i e-distribucije su vrlo slični. Razlikuju se po tržišnom fokusu, tako da se onlajn prodaja u B2C sektoru fokusira na prodaju individualnim kupcima, dok se u slučaju e-distribucije model fokusira na prodaju drugim kompanijama. Na klasifikaciju biznis modela utiče i vrsta tehnološke osnove na kojoj se obavlja e-trgovina. Npr. model onlajn prodaje se može primeniti i na m-trgovinu, zasnovanu na bežičnoj tehnologiji, ali je jasno da specifičnosti ove tehnologije zahtevaju prilagođavanje odgovarajućih biznis modela. Pojedine kompanije, kao npr. eBay.com, koriste višestruke biznis modele. eBay.com se može posmatrati i kao B2C kreator tržišta i kao C2C biznis model. Uz dopuštanje učešća na aukcijama pomoću mobilnih telefona, eBay.com se može posmatrati i kao kompanija koja je razvila i m-komerc biznis model. U Tabeli 2.3.1 dat je pregled osnovnih B2C poslovnih modela.

B2C POSLOVNI MODELI				
Poslovni model	Varijacije	Primeri	Opis	Model prihoda
Portal	Horizontalan/ opšti	Yahoo.com AOL.com MSN.com	Nudi integrisani paket servisa pretraživanja, vesti,e-maila, četa, preuzimanja muzičkih i video sadržaja, kalendara i td. Pretenduje da bude home page što većem broju korisnika	Reklamiranje, pretplate, transakcione provizije
	Verikalan/ specijalizovan (Vortal)	Salient.com	Nudi servise i proizvode u okviru specijalizovanog segmenta tržišta	Reklamiranje, pretplate, transakcione provizije
E-tejler	Virtuelna prodavnica	Amazon.com	Onlajn verzija prodavnice u kojoj se kupuje u bilo koje doba dana i noći bez napuštanja kuće ili posla	Prodaja proizvoda
	Klik i Brik	Wal-Mart.com Sears.com	Onlajn distribucioni kanali kompanije koja ima i fizičke prodavnice	Prodaja proizvoda
	Kataloška prodaja	LandEnd.com LLBean.com	Onlajn verzija kataloške prodaje	Prodaja proizvoda
	Direktno od proizvođača	Dell.com Compaq.com		Prodaja proizvoda

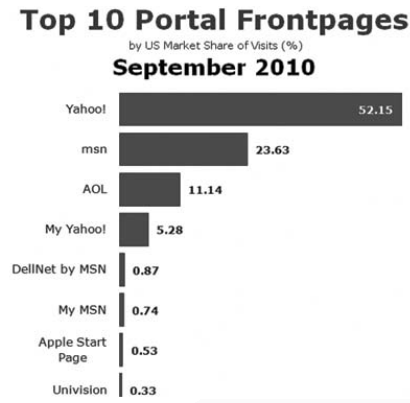
(nastavak na sledećoj strani)

Poslovni model	Varijacije	Primeri	Opis	Model prihoda
Transakcioni brokeri		E-Trade.com Expedia.com Monster.com Travelocity.com Hotels.com Orbitz.com	Izvršavanje onlajn prodajnih transakcija. Obuhvataju berzanske brokere i putničke agente. Transakcije se obavljaju brže i jeftinije	Transakcione provizije
Kreatori tržišta	Aukcije	Ebay.com Priceline.com Amazon.com	Web zasnovano poslovanje u cilju kreiranja tržišta na kome se susreću kupci i prodavci	Transakcione provizije
Servis provajderi		Lawinfo.com myCFO.com	Kompanije koje prodaju servise	Prodaja servisa
Provajderi okupljanja		About.com Ivillage.com NetNoir.com Oxygen.com Epinions.com	Sajtovi koji omoguavaju okupljanja i razmenu ideja i iskustava ljudi sličnih interesovanja i hobija	Reklamiranje, pretplate, afilacione provizije

Tabela 2.3.1 Pregled osnovnih B2C poslovnih modela

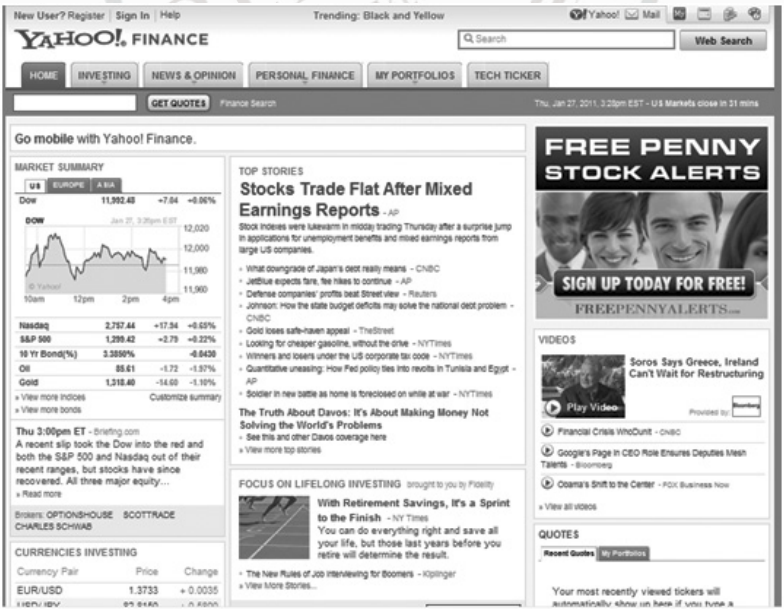
2.3.1 Portali

Portali su Web sajtovi koji nude posetiocima na jednom mestu snažne pretraživače Web stranica, zajedno sa integrisanim paketima sadržaja i servisa tipa novosti, e-maila, sistema za razmenu poruka, kalendara, elektronske trgovine, distribucije audio i video sadržaja i td. U početku razvoja Weba posmatrani su kao ulazne tačke Interneta, dok su danas evoluirali u destinacione sajtove na kojima možete da zadovoljite većinu vaših potreba vezanih za Web servise. Marketinški se označavaju kao mesta na kojima posetilac započinje Web pretragu i ostaje duži vremenski period čitajući vesti, pregledajući e-mail poruke, nalazeći zabavne sadržaje i kontaktirajući druge ljude. Na portalima se ništa ne prodaje direktno i u tom pogledu zadržavaju imidž nepristrasnog informisanja potencijalnih kupaca. Finansijski model portala se bazira na reklamiranju, afilacionim provizijama od usmeravanja kupaca ka referisanim sajtovima e-trgovine, kao i od pretplata za različite varijante premijum servisa. Neki od portala, kao npr AOL i MSN su istovremeno i Internet provajderi, što dodatno upotpunjuje finansijsku komponentu poslovnog modela.



Sl.2.3.1 Prikaz 10 najposećenijih portala na Američkom tržištu u septembru 2010 godine. Izvor www.marketingcharts.com

Podaci sa Sl.2.3.1 pokazuju da prva tri najposećenija portala na Američkom tržištu privlače gotovo 87% svih Internet korisnika. Yahoo, AOL, MSN i drugi portali o kojima je do sada bilo reči su tzv. horizontalni portali, budući da im je cilj privlačenje svih korisnika Interneta. Za razliku od njih, vertikalni portali, koji se često nazivaju i vortali, imaju za cilj privlačenje što većeg broja korisnika Interneta određenog interesovanja ili određenog segmenta tržišta.



Sl.2.3.2 Finansijski vortal YahooFinance

2.3.2 E-tejleri

Onlajn maloprodaja, poznata i pod nazivom e-tejler, se pojavljuje u svim oblicima i veličinama, od gigantskog Amazon.com do malih lokalnih prodavnica koje imaju svoje Web sajtove. E-tejleri su vrlo slični klasičnoj fizičkoj maloprodaji, za razliku od koje kupci pristupaju Web sajtu, pregledaju kataloge ponuđenih proizvoda i vrše naručivanje. E-tejleri tipa "clicks & bricks" su zamena za postojeće fizičke prodavnice i nude iste proizvode. JCPenney, Barnes&Noble i Wal-Mart su primeri kompanija sa komplementarnim onlajn prodavnicama. Postoje i varijante e-tejlera koje su onlajn verzija kataloške prodaje poštom, kao i varijanta direktne prodaje od proizvođača.

U ovom sektoru je izuzetno velika konkurencija s bzirom an vrlo nisku ulaznu barijeru. Pod ulaznom barijerom se podrazumevaju ukupni troškovi ulaska na novo tržište. Stoga je opstanak i profitabilno poslovanje veoma teško postići u ovom sektoru, ukoliko se ne poseduje prethodno iskustvo ili već formirani brend. Kompanije koje teže da dođu do svakog onlajn kupca će sa velikom verovatnoćom brzo iscrpeti sve svoje resurse. Stoga kompanije koje razvijaju strategiju niša, jasno definišući ciljno tržište i njegove potrebe, po pravilu su i najbolje pripremljene za profitabilno poslovanje. Ključni faktori uspeha u ovom sektoru su pažljivi odabir ponude, zadržavanje troškova na niskom nivou i kontrola zaliha.

2.3.3 Dostavljači sadržaja

Provajderi sadržaja vrše distribuciju informacionih sadržaja, kao što su digitalne vesti, muzika, fotografije, video i umetnička dela pomoću Internet tehnologije. Preuzimanje i plaćanje digitalnih sadržaja je drugi po veličini izvor prihoda u B2C sektoru. Finansijski model se zasniva na pretplati. Npr. Rhapsody.com na osnovu mesečnih pretplata omogućava članovima pristup digitalnim muzičkim sadržajima. WSJ.com (Wall Streat Journal onlajn), Harvard Business Review i mnogi drugi, naplaćuju preuzimanje sadržaja po pojedinačnom pristupu ili u kombinaciji sa pretplatom. Ovaj sektor je pokrenuo razvoj sistema za mikroplaćanja, kao npr Qpass sistem, koji je efikasan sistem naplate iznosa između $0.25 i $5.00. Pojava ovih sistema je značajno unapredila model prihoda kompanija čiji se biznis model zasniva na ponudi digitalnih sadržaja. Osim ove klase, postoji čitav skup dostavljača digitalnih sadržaja koji ne naplaćuju svoje usluge, kao što su CIO.com, CNN.com itd. Njihov finansijski model se zasniva na reklamiranju i promociji partnerskih (afilacionih) sajtova.

Ključ uspeha kompanija koje distribuiraju digitalne sadržaje je posedovanje sadržaja koji imaju tržišnu vrednost. Tradicionalni vlasnici sadržaja, kao što su izdavači novina i knjiga, filmske kompanije, radio i televizijske kompanije i mreže imaju ogromnu prednost nad novim onlajn kompanijama iz istog sektora. Stoga veliki broj onlajn distributera ne poseduje sadržaj koji distribuiraju, već svoj finansijski model zasnivaju na agregaciji i

distribuciji sadržaja u ime onih koji imaju vlasništvo nad njima. Naravno da je moguće da i nove onlajn kompanije u ovom sektoru naprave uspeh, ali je to vezano dominantno za posedovanje jedinstvenog sopstvenog izvora informacionih sadržaja odgovarajuće tržišne vrednosti.

2.3.4 Transakcioni brokeri

Sajtovi koji obavljaju transakcije koje se normalno obavljaju lično, telefonom ili poštom, nazivaju se transakcioni brokeri. Oblasti u kojima se najčešće koristi ovaj model poslovanja su finansijki servisi, servisi putovanja i ponude i potražnje radnih mesta. Vrednost koju nude tržištu je ušteda sredstava i vremena. Osim toga u ponudi transakcionih brokera su i različite informacije i istorijski podaci, kao i stručni saveti i mišljenja. Npr. onlajn transakcioni berzanski brokeri, kao što su E-Trade.com, Ameritrade.com i Schwab.com zauzimaju preko 20% od ukupnog broja berzanskih transakcija. Korisnike privlače nižim cenama po transakciji od klasičnih berzanskih brokera, uz čitav niz dodatnih povoljnosti i popusta. Međutim, prelaz sa klasičnih na onlajn brokere, praćen je velikim nepoverenjem korisnika, kako u pogledu privatnosti i sigurnosti, tako i gubitka ličnog kontakta sa fizičkim brokerima koji su uz svoje standardne servise usput uvek nudili i prijateljske savete u vezi obavljanja pojedinih transakcija. Stoga onlajn brokeri moraju posebno obratiti pažnju i uveriti svoje klijente u visok stepen ostvarene privatnosti ličnih finansijskih podataka, sigurnost obavljenih transakcija, a uvođenjem dodatnih servisa pokušati da supstituišu nedostajući lični kontakt sa klijentom.

2.3.5 Kreatori tržišta

Kreatori tržišta grade digitalno virtuelno okruženje u kome se susreću kupci i prodavci, izlažu i pretražuju proizvodi i na kraju uspostavlja prihvatljiva cena. Pre pojave Interneta i Weba, kreatori tržišta su ovo mogli postići samo oslanjanjem na fizički prostor i vremensko prostorni susret kupaca i prodavaca. Pojava Weba je omogućila separaciju tržišta od fizičkog prostora. Dobar primer je kompanija Priceleine.com, koja omogućava korisnicima da postave svoje cene koje su spremni da plate za različite servise vezane za putovanja, kao što su smeštaj i transport. Ovakav model se naziva još i model inverzne aukcije. Kompanija eBay.com je ustvari onlajn aukcioni sajt, koji pruža usluge i pojedincima i preduzećima. Aukcioni biznis model eBay.com kreira digitalno okruženje za susret kupaca i prodavaca, koji se zatim dogovaraju o cenama i obavljaju poslovne transakcije. Zapazimo razliku u odnosu na transakcione brokere, koji obavljaju poslovne transakcije u ime svojih klijenata kao agenti na širem tržištu. Na eBay.com kupci i prodavci su svoji sopstveni agenti. Svaka transakcija donosi eBay.com odgovarajuću proviziju. Ova kompanija je jedna od retkih onlajn kompanija koja je od samog pošetka rada profitabilna. Ključ uspeha leži u činjenici da je eBay.com jednostavno posrednik, koji nema ni

proizvodnih troškova ni troškova skladištenja proizvoda. Očekivano tržište za kompanije iz ovog sektora je izuzetno veliko, ali pod uslovom da se raspolaže sa finansijskim sredstavima za privlačenje dovoljno velikog broja kupaca i prodavaca. Krajem 2008. godine ova kompanija je imala nekoliko stotina miliona korisnika, 15 000 zaposlenih i zaradu od 7,7 milijardi dolara. Nove kompanije koje ulaze na ovo tržište moraju da nastupe sa agresivnim brendiranjem i programima podizanja svesti i saznanja u cilju privlačenja kritične mase korisnika. Amazon.com je iskoristio svoju ogromnu bazu podataka o kupcima za starovanje sopstvene prodaje zasnovane na aukcijskom modelu. Neke druge kompanije iz ovog sektora su u cilju opstanka na tržištu, divresifikovale poslovanje u niz manjih specijalizovanih vertikalnih tržišnih segmenata, kao što su npr. nakit i automobili.

2.3.6 Servis provajderi

Kao što e-tejleri prodaju proizvode onlajn, na isti način servis provajderi nude servise onlajn. Za uzvrat ili naplaćuju isporučeni servis ili ostvaruju prihod na posredan način, kao što je reklamiranje ili prikupljanje ličnih podataka korisnih za direktni marketing. Mnogi servisi se ne mogu prodavati onlajn, kao što su npr. popravka automobila ili vodovodnih instalacija, ali i u tom slučaju se ceo aranžman popravke može obaviti onlajn. Spektar servisa u onlajn ponudi je izuzetno raznolik: od ponude memorijskog prostora, kao što su Dropbox.com Box.net.com, poslovnih saveta, kao što je Business-thinking.com, pa do pretraživača Web sadržaja, kao što su Google.com i Yahoo.com. Osnovna ponuda vrednosti servis provajdera je vredna, pogodna, brza i jeftina alternativa tradicionalnih servis provajdera ili u slučaju pretraživača, ponuda servisa pretrage koji je zaista jedinstven na Webu. Finansijski model servis provajdera se sastoji od modela pretplate, naplata jednokratne upotrebe nekog servisa ili provizija od prodaje ili dostave kupljenih proizvoda. Očekivano tržište u ovom sektoru je veliko koliko i sva raznolikost ponuđenih servisa i potencijalno je veliko koliko i tržište fizičkih proizvoda. Na ruku ovom sektoru ide činjenica da je savremena ekonomija i društvo u celini servisno orjentisano i da neprekidno raste potreba savremenog čoveka za sve većim brojem servisa, od servisa brze hrane, brze dostave paketa i pošte, pa do čitavog niza servisa mobilne telefonije. Marketinške akcije servis provajdera treba da budu usmerene na prevazilaženje straha kupaca od unajmljivanja provajdera onlajn putem, sticanje poverenje među sadašnjim i budućim korisnicinma, kao i navođenje potencijalnih kupaca da isprobaju ponuđene servise.

2.3.7 Provajderi okupljanja

Provajderi okupljanja su sajtovi koji kreiraju digitalno onlajn okruženje (društvenu mrežu) za okupljanje ljudi sličnih interesa u cilju obavljanja transakcija kupovine ili prodaje, komuniciranja sa istomišljenicima, dobijanja informacija iz domena zajedničkog

interesovanja ili čak preuzimanja onlajn virtuelnog identiteta u cilju igre ili slobodnog fantaziranja. Osnovna ponuda vrednosti provajdera okupljanja je kreiranje brzog i funkcionalnog sajta na kome se korisnici mogu fokusirati na svoje najznačajnije zajedničke interese i probleme. Oslanjaju se po pravilu na hibridni model prihoda, koji obuhvata pretplatu, prodaju, transakcione provizije, afilacione provizije i prihode od oglašavanja kompanija koje su privučene fokusiranim profilom korisnika datog sajta. Najpoznatije današnje društvene mreže su Facebook, MySpace i Linkedln.

Sl.2.3.3 Sajt Epinions.com pripada sektoru provajdera okupljanja. Osnovu za okupljanje predstavlja pisanje i čitanje ocena i prikaza proizvoda široke potrošnje

Važan zahtev u vođenju sajtova okupljanja je kompetentan i iskusan menadžerski tim koji je u stanju da usmerava i vodi zajednicu na kompetentan i nenametljiv način. Nedostatak iskusnog personala može značajno da spreči rast zajednice, koja ima potrebu za menadžerima i medijatorima sposobnim da održavaju diskusije odgovarajuće forme i sadržaja. Interes za onlajn zajednicama raste, a samim tim i potencijalno tržište provajdera okupljanja. Ključan elemenat uspeha je pronalaženje dobro definisane tržišne niše koja još uvek nije zauzeta nekim provajderom okupljanja. Dobra je ideja startovati od malih segmenata tržišta koji ne privlače pažnju velikih igrača, čime se izbegava direktna konkurencija u osetljivom početnom periodu razvoja. Najveći izazov predstavlja balans između cene kvaliteta ponuđenog sadržaja i prihoda koji se mogu ostvariti reklamiranjem. U pogledu marketinških kampanja, za ovaj sektor je najbitnije nagovoriti korisnike da se pridruže onlajn zajednici. Što je zajednica veća, povećavaju se provizije od reklamiranja i prihodi od prodaje preko afilacionih sajtova.

2.4 NAJVAŽNIJI B2B POSLOVNI MODELI

Kao što smo već napomenuli u prvom poglavlju, B2B sektor donosi prihode koji su za jedan red veličine veći od B2C sektora. U 2010. godini oni su iznosili za američko tržište 3800 milijardi dolara prema 230 milijardi dolara. U Tabeli 2.4.1 dat je pregled najvažnijih B2B biznis modela.

B2B POSLOVNI MODELI – MREŽNO TRŽIŠTE			
POSLOVNI MODEL	PRIMERI	OPIS	MODEL PRIHODA
E-distributeri	Grainger.com FindMRO.com Staples.com	Onlajn verzija maloprodaje i veleprodaje, održavanje sanbdevanja, popravke, indirektni ulazi	Prodaja proizvoda
E-nabavke	Ariba.com CommerceOne.com Siemens	Pojedinačne kompanije koje kreiraju digitalno tržište na kome kupci i prodavci obavljaju transakcije nad indirektnim ulazima	Provizije za pružanje usluga posrednika, prihodi od upravljanje zalihama i servisima obavljanja transakcija
Berze	Exchange.eSteel.com IMX.com GEPolymerland.com	Nezavisna digitalna tržišta nad direktnim ulazima. Vertikalna industrijska orjentacija	Provizije od transakcija
Industrijski konzorcijumi	Covisint.com Sciquest.com Pasticsnet.com	Vertikalna digitalna tržišta u posedu industrije namenjena selekciji snabdevača	Provizije od transakcija

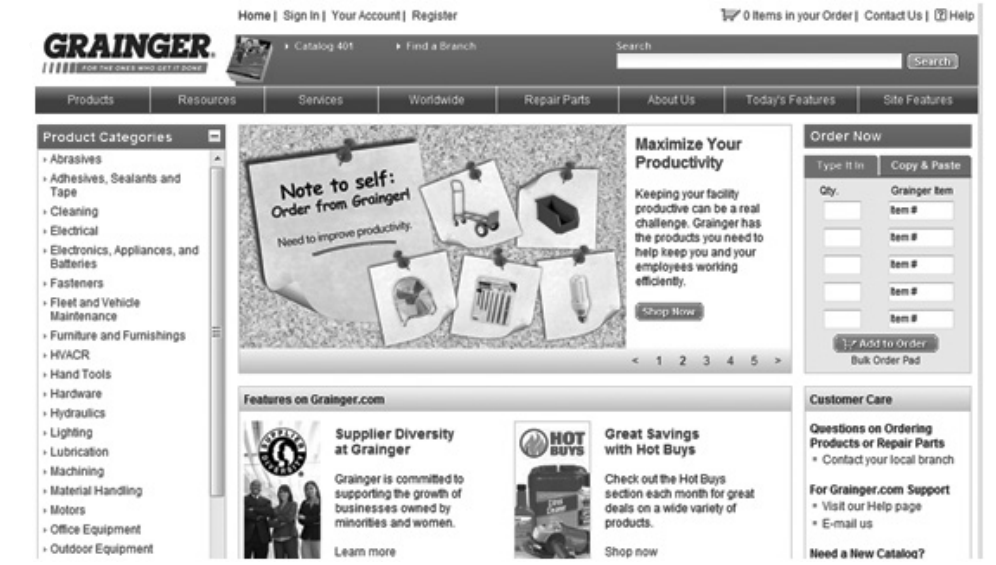
Tabela 2.4.1 Najvažniji B2B poslovni modeli tipa mrežnog tržišta

B2B POSLOVNI MODELI – PRIVATNE INDUSTRIJSKE MREŽE			
POSLOVNI MODEL	PRIMERI	OPIS	MODEL PRIHODA
Mreža pojedinačne kompanije	Wal-Mart Proctor&Gamble DaimlerChrysler Ford Motor Co.	Mreža u vlasništvu jedne kompanije za kordinaciju lanca snabdevanja od ograničenog broja partnera	Troškove pokriva kompanija-vlasnik, a nadoknada troškova se zasniva na efikasnijoj distribuciji i proizvodnji
Mreža na nivou industrijskih grana	Nistevo Inc. Globalnextchange.com UCCnet.org Worldwideretailexchange.org	Mreža u vlasništvu industrijskih grana namenjena postavljanju standarda, koordinacije snabdevanja i logistike	Troškove pokrivaju kompanije članovi industrijskih grana, a nadoknada troškova se zasniva na efikasnijoj distribuciji i proizvodnji; provizije od transakcija i servisa

Tabela 2.4.2 Najvažniji B2B modeli poslovanja tipa privatnih mreža

2.4.1 E-distributeri

Pod e-distributerima se smatraju kompanije koje snabdevaju proizvodima i servisima pojedinačne kompanije. Kritičan faktor uspeha ovih kompanija je veličina i raznovrsnost ponude. Što je veći broj proizvoda i servisa u ponudi na Web sajtu ovih kompanija, to su one atraktivnije za potencijalne kupce. Poznato je da tzv „one stop" kupovina, odnosno kupovina svih potrebnih proizvoda i servisa na jednom mestu je uvek kod kupaca ispred kupovine koja zahteva pretragu i kupovinu na više različitih sajtova. Dobar primer je kompanija Grainger, koja je startovala svoje online poslovanje u B2B sektoru 1995. godine. Danas se na sajtu ove kompanije mogu naći ponude za preko 400 000 različitih proizvoda uključujući sredstva za održavanje brodova i vozila, alate, proizvode iz domena obezbeđenja i zaštite, motore, sredstva za čišćenje, proizvode za vodovodne, grejne i ventilacione sisteme i td. Grainger nudi i mnoge besplatne servise, kao što su upravljanje zalihama, revizija projekata osvetljenja, obuka obezbeđenja, priprema za programe održivosti i vanrednih situacija i td. Popusti su po pravilu između 10% i 48%, a dostava je besplatna u toku narednog dana, ukoliko je narudžba kompletirana do 16 sati prethodnog dana, videti sl.2.4.1.



Sl.2.4.1 Web sajt kompanije Grainger koja spada u grupu e-distributera sa preko 400 000 proizvoda u ponudi.

Interesantan je poslovni model Geae.com sajta, koji je u stvari kompanija u okviru General Electric Aircraft Engines (GEAE) kompanije. Naime GEAE je veliki kupac delova za avionske motore. S druge strane, zbog dominantne uloge ove kompanije u sektoru avionskih motora, jasno je da će i mnoge druge kompanije kupovati iste proizvode ako ih

kupuje GEAE. Stoga je na geae.com instaliran sistem za nabavke kome mogu pristupiti i poslovni partneri GEAE, a objedinjavanjem zajedničkih narudžbi postižu se značajni popusti. Postavljajući se na taj način kao fokusna tčka u svim većim kupovinama GE je poboljšao svoju kupovnu moć i poslovnu povezanost. Na ovaj način je kreiran još jedan profitni centar u okviru GE uz istovremeno redukovanje sopstvenih troškova poslovanja.

2.4.2 E-nabavke

Kao što e-distributeri obezbeđuju proizvode drugim kompanijama, B2B e-nabavljači kreiraju i prodaju pristup digitalnim elektronskim tržištima. Kompanije, kao što su Ariba.com na primer, kreiraju softver koji pomaže velikim kompanijama da organizuju proces nabavki tako što se kreira mini digitalno tržište za jednu kompaniju. Ariba kreira prilagođeni integrisani onlajn katalog, u okviru koga kompanije snabdevači mogu da prikažu svoje proizvode za potrebe kompanija koje kupuju. Na strani prodavaca Ariba pomaže u kreiranju kataloga, isporuci, osiguranju i finasijama. Softver sa strane kupca i prodavca se označava generički kao softver za upravljanje lancem vrednosti.

B2B servis provajderi zarađuju na osnovu transakcionih provizija, broja računara na kojima je instaliran njihov softver ili na osnovu prodaje godišnjih licenci. Kompanijama koje kupuju nude sofisticirani softver za upravljanje lancima snabdevanja, čime se u značajnoj meri redukuju troškovi. U softverskim krugovima kompanije kao što su Ariba ili CommerceOne se nazivaju provajderi aplikacionih servisa –ASP (Application Service Providers).

2.4.3 B2B habovi

B2B habovi ili berze su digitalna elektronska tržišta na kojima se susreće veliki broj dobavljača i mali broj velikih komercijalnih kupaca. B2B habovi su vlasništvo nezavisnih preduzetničkih kompanija, koje zarađuju na osnovu provizija po svakoj obavljenoj transakciji. Po pravilu rade u okviru jedne vertikalne industrijske grane, kao što su čelik, polimeri, aluminijum i drugo. Za kupce B2B habovi omogućavaju dobijanje na jednom mestu najnovijih informacija o dobavljačima, cenama i ostalim relevantnim podacima. Za prodavce B2B habovi su značajni zbog lakšeg pristupa kupcima. Što je veći broj kupaca i prodavaca, niži su troškovi prodaje i veća verovatnoća obavljanja prodaje. Lakoća, brzina i obim izvršavanja transakcija se sumarno naziva likvidnost tržišta. Teorijski, B2B habovi čine mnogo jeftinijim proces identifikacije potencijalnih dobavljača, kupaca i partnera i obavljanja transakcija. Kao rezultat imamo smanjenje transakcionih troškova – troškova obavlajnja prodaje ili kupovine. B2B habovi smanjuju i troškove proizvodnje i skladištenja proizvoda.

2.4.4 Industrijski konzorcijumi

Industrijski konzorcijumi su vertikalna tržišta u vlasništvu date industrijske grane, koja služe potrebama specifičnih industrijskih grana kao što su automobilska, aeronautička, hemijska, drvna industrija i sl. Vertikalna tržišta snabdevaju manji broj kompanija proizvodima i servisima specifičnim za pojedine industrijske grane, dok horizontalna tržišta snabdevaju kompanije iz različitih industrijskih grana specifičnim proizvodima i uslugama, kao što su marketinške, finansijske ili informatičke. Jedan od najvećih vertikalnih B2B industrijskih konzorcijuma je Covisint, berza auto delova podržana od Daimler-Chryslera, Forda, General Motorsa, Renoa, CommerceOne i Oracla. Cilj Covisinta je pomoć automobilskoj industriji u povećanju efikasnosti lanaca snabdevanja kreiranjem digitalnog tržišta i pojačanom koordinacijom među kupcima i prodavcima. Industrijski konzorcijumi su po pravilu uspešniji od nezavisnih berzi, delom zbog moćnih sponzora u datim industrijskim granama, kao i pristupa jačanja tradicionalnih kupovnih navika umesto težnje da se one promene.

2.4.5 Privatne industrijske mreže

Privatne industrijske mreže su digitalne mreže, namenjene koordinaciji komunikacionih tokova između kompanija angažovanih na zajedničkom poslu. Na primer Wal-Mart održava jednu od najvećih na svetu privatnih industrijskih mreža za potrebe njenih dobavljača, koji dnevno koriste ovu mrežu za praćenje prodaje njihovih proizvoda, status dostave i nivoe zaliha. Oko 70% celokupne B2B e-trgovine koristi stariju tehnologiju koja se naziva EDI – Electronic Data Interchange. EDI je koristan za pojedinačne relacije između dobavljača i kupaca. Prvobitno je dizajniran za zatvorene mreže, ali smo svedoci brze migracije ove tehnologije na Internet infrastrukturu. Web tehnologija zamenjuje EDI zbog mogućnosti podržavanja tržišnih odnosa tipa "više prema jednom" i „više prema više", gde više dobavljača prodaje jednoj ili grupi velikih kupaca ili kao u slučaju B2B habova, gde na tržištu istovremeno postoji i više prodavaca i više kupaca. EDI nije namenjen za podržavanje ovih složenijih tržišnih odnosa. Postoje dve vrste privatnih industrijskih mreža: mreže jedne kompanije ili mreže vezane za celokupnu industrijsku granu.

Mreže jedne kompanije su najčešća forma privatnih industrijskih mreža. Po pravilu su u vlasništvu velikih kompanija koje imaju potrbu za intezivnom kupovinom, kao što su Wal-Mart ili Chrysler. Particpiraju samo kompanije po pozivu, koje su stekle poverenje na osnovu dugogodišnjeg poslovanja. Po pravilu nastaju evolucijom kompanijskih ERP (Enterprise Resource Planning) sistema izvan kompanijskih granica. Na ovaj način se ključni snabdevači date kompanije uključuju u jedinstven kompanijski sistem donošenja poslovnih odluka. Tako na primer, DajmlerKrajslerov SPIN (Supply Partner Information Network) sistem omogućava da preko 20 000 dobavljača sa 3 500 različitih lokacija širom sveta, pristupaju sistemu za prognozu potreba i nabavki na dnevnoj osnovi. Na osnovu

ovih informacija, dobavljači planiraju sopstvenu produkciju, isporuku i praćenje delova i izvršenje naplate.

Mreže na nivou industrijskih grana nastaju evolucijom industrijskih asocijacija. Vlasništvo su konzorcijuma velikih kompanija u okviru jedne industrijske grane, sa ciljem da postavljaju neutralne standarde za komercijalne komunikacije na Internetu, poseduju otvorenu ili zajedničku tehnološku platformu za rešavanje industrijskih problema, i međusobno komuniciranje u cilju rešavanja zajedničkih problema.

2.5 POSLOVNI MODELI U DOMENU E-TRGOVINE U NASTAJANJU

Uobičajene forme e-trgovine obuhvataju B2C i B2B modele. Međutim razvoj Weba doveo je do pojave novih oblika poslovanja, kao što su C2C, P2P i M-komerc. U tabeli 2.5.1 dat je pregled ovih poslovnih modela koji se sve češće susreću na ovim tržištima u nastajanju.

POSLOVNI MODELI U DOMENU E-TRGOVINE U NASTAJANJU				
Poslovni model	Model	Primer	Opis	Model prihoda
C2C	Kreatori tržišta	eBay.com Half.com	Pomaže korisnicima da se povežu sa drugim korisnicima u cilju međusobnog trgovanja	Transakcione provizije
P2P	Provajderi sadržaja	Kazaa.com Groovenet works.com	Tehnologija deljenja fajlova i servisa pomoću Weba bez zajedničkog servera	Pretplate, reklamiranje, transakcione provizije
M-trgovina	Različiti	Armani Skyline Chili	Proširenje poslovnih aplikacija na bežičnu tehnologiju	Prodaja roba i usluga

Tabela 2.5.1 Prikaz osnovnih poslovnih modela e-trgovine u nastajanju

2.5.1 C2C poslovni modeli

C2C model omogućava pojedincima prodaju jedni drugima na osnovu onlajn digitalne tehnologije. Prvi i najbolji primer ovog tipa poslovanja je eBay.com, koji primenjuje poslovni model kreatora tržišta. Pre pojave eBay.com jedina mogućnost za obavljanje trgovine ovog tipa su bile buvlje pijace za izlaganje i kupovinu korišćene robe. Pojavom

onlajn aukcija, otpala je potreba da kupci moraju da napuštaju svoje kuće i poslove, a prodavci da rentiraju prostor za izlaganje proizvoda. Finansijski model eBay.com su provizije od obavljenih transakcija. Kupci koji žele da kupuju korišćene proizvode a ne vole aukcije, mogu da koriste Half.com, na kome prodavci fiksiraju cene proizvoda.

2.5.2 P2P poslovni modeli

Na sličan način kao u C2C modelu, P2P poslovni model povezuje korisnike omogućavajući deljenje zajedničkih fajlova i računarskih resursa bez zajedničkog servera. Osnovni cilj P2P kompanija je pomoć korisnicima da učine svoje digitalne sadržaje raspoložive svima ostalim korisnicima Weba. Na samom početku razvoja ovog poslovnog modela, P2P sistemi su korišćeni za nelegalnu razmenu muzičkih sadržaja na Internetu. Izazov u narednim fazama razvoja je formiranje takvog poslovnog modela koji će na istim tehnološkim osnovama obezbeđivati legalne prihode. Jedna grana razvoja P2P poslovnih modela je korišćenje ove tehnologije za koordinaciju rada u kompanijama. Groovenetworks.com je razvio klijentski i severski softver koji pomaže zaposlenima unutar jedne kompanije da dele fajlove, kalendare, radne rasporede i planove bez opterećivanja centralnog server. Međutim i dalje je dominantna uloga ovih modela u deljenju zajedničkih video i muzičkih sadržaja, kao što je to ostvarila kompanija Kazaa.com, uz sve probleme delovanja u legalnim okvirima i ne naršavanja zakona o autorskim pravima.

2.5.3 Poslovni modeli u M-poslovanju

M-trgovina je skraćenica za mobilnu trgovinu. Zasniva se na tradicionalnim e-komerc modelima podržanim novim mogućnostima bežičnog Interneta i mobilnih terminalnih uređaja kao što su mobilni telefoni i PDA uređaji. Osnovna prednost ovog modela je pristup Internetu u bilo koje vreme na bilo kom mestu, pomoću mobilnih terminalnih uređaja. Ključne tehnologije su 3G mobilni telefoni, Wi-Fi bežične lokalne računarske mreže i Bluetooth, bežična komunikacija na kratkim rastojanjima zasnovana na radio prenosu. Sve pomenute tehnologije su u eksplozivnom rastu. U svetu danas ima više korisnika mobilne telefonije nego Internet korisnika, što otvara mogućnost profitabilnog prenosa postojećih Web baziranih poslovnih modela na mobilne telefone. Trenutno je u upotrebi oko 285 miliona bežičnih telefona u Sjedinjenim Državama, što predstavlja gotovo 91% ukupne populacije. Na svetskom nivou broj korisnika mobilnih telefona iznosi 5 milijardi ili oko 67% ukupne svetske populacije [3]. Prodaja u okviru m-trgovine dostigla je u Sjedinjenim Državama $1.2 milijarde u 2009, odnosno $2.42 milijarde u 2010. godini [4]. I pored ovog rapidnog trenda rasta, istraživanja pokazuju da 62% B2C kompanija ne planiraju još uvek uvođenje mobilne strategije prodaje [5]. Ovaj pokazatelj svedoči o tome da uvođenje m-trgovine nije jednostavno prenošenje Web sajta dizajniranog za klasičnu e-trgovinu u okruženje mobilnih bežičnih mreža. Onlajn kupci su

izuzetno osetljivi na bilo kakve manjkavosti brzog pretraživanja onlajn sadržaja. U tom pogledu m-trgovina je u mnogo težem položaju od klasične onlajn trgovine, budući da su mali ekrani mobilnih uređaja i trenutno stanje propusnog opsega mobilnih mreža ograničavajući faktori u brzom i preglednom pretraživanju m-komerc Web sajtova. Stoga se po pravili dizajniraju posebni Web sajtovi prilagođeni zahtevima mobilnih klijenata, kao što su lakše učitavanje stranica, lakše sleđenje linkova, manje opterećenje grafičkim sadržajima koji zahtevaju veliku količinu podataka, lakše i preglednije pretraživanje na malim ekranima, preciznija navigacija i lokacija pomoću opštih pretraživača.

2.5.4 Podrška e-poslovanju

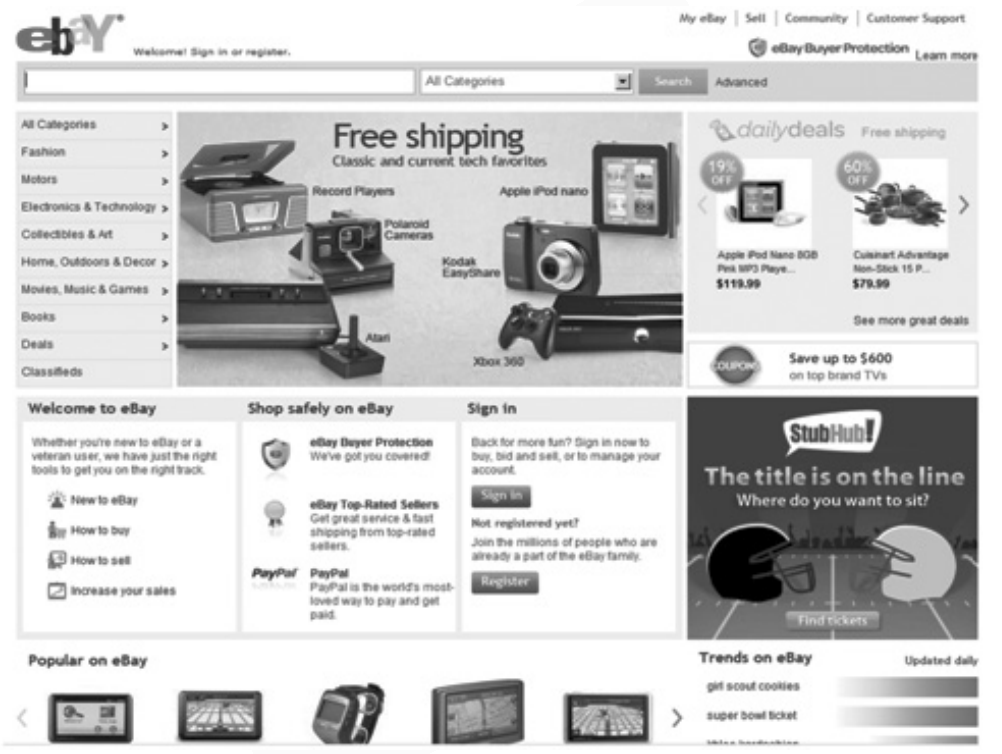
Kompanije čiji je primarni cilj infrastrukturna podrška e-trgovini čine poseban privredni sektor čija je poslovna sudbina u tesnoj vezi sa e-poslovanjem i njegovim razvojem. One obezbeđuju hardver, operativne sisteme, mrežnu i telekomunikacionu opremu, aplikativni softver, Web dizajn, sve vrste konsultacionih servisa i ostale proizvode i usluge koje omogućavaju uspešno onlajn poslovanje, Tabela 2.5.2.

PODRŠKA E-POSLOVANJU	
INFRASTRUKTURA	KOMPANIJE
Hardver: Web serveri	IBM,HP/Compaq, Dell, Sun
Softver: operativni sistemi i serverski softver	Microsoft, RedHat Linux, Sun, Apache Software Foundation
Mreže: ruteri	Cisco, JDS Uniphase, Lucent
Sigurnost: Softver za šifrovanje	VeriSign, Check Point, PGP Corporation
Sistemi za e-trgovanje (B2C, B2B)	IBM, Microsoft, CommerceOne, Ariba, BroadVision
Rešenja za striming medije	Real Networks, Microsoft, Apple
Softver za upravljanje odnosima sa kupcina	PeopleSoft, Siebel, SAP
Platni sistemi	Verisign, PayPal, CyberCash
Poboljšanje performansi	Akamai, Cache Flow, Inktomi, Cidera
Baze podataka	Oracle, IBM,Microsoft, Sybase
Servisi hostovanja	Interland,IBM, WebIntellects

Tabela 2.5.2 Infrastrukturna podrška e-trgovini

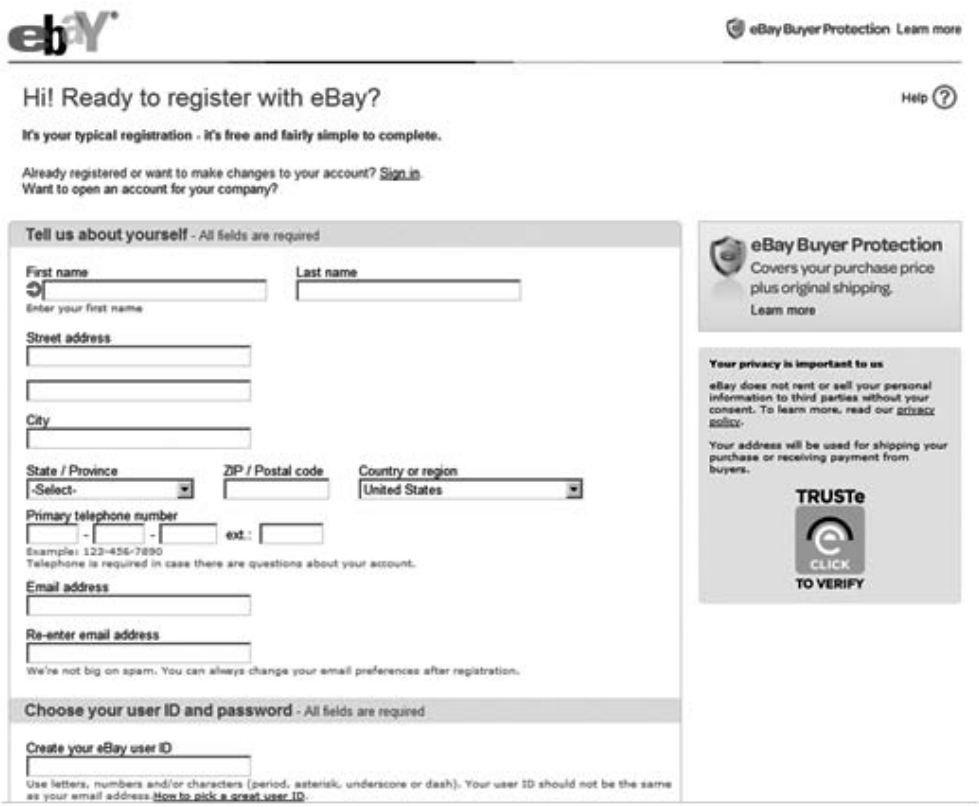
2.5.5 Studija slučaja: eBay.com

Web adresa www.eBay.com je jedna od najpopularnijih Web adresa, na kojoj se dnevno odvija preko milion aukcija. Sa bazom od nekoliko stotina miliona korisnika eBay predstavlja jedno od najvećih tržišta za kupovinu svega i svačega. Web sajt je započeo sa radom 1995. godine radi razmene PEZ figurica. eBay omogućava prodaju na lokalnom, nacionalnom i internacionalnom nivou. Velike međunarodne kompanije, kao IBM, prodaju svoje najnovije proizvode i nude usluge na eBay-u koristeći konkurentnost aukcijskog modela prodaje.



Sl.2.5.1 Početna stranica eBay.com

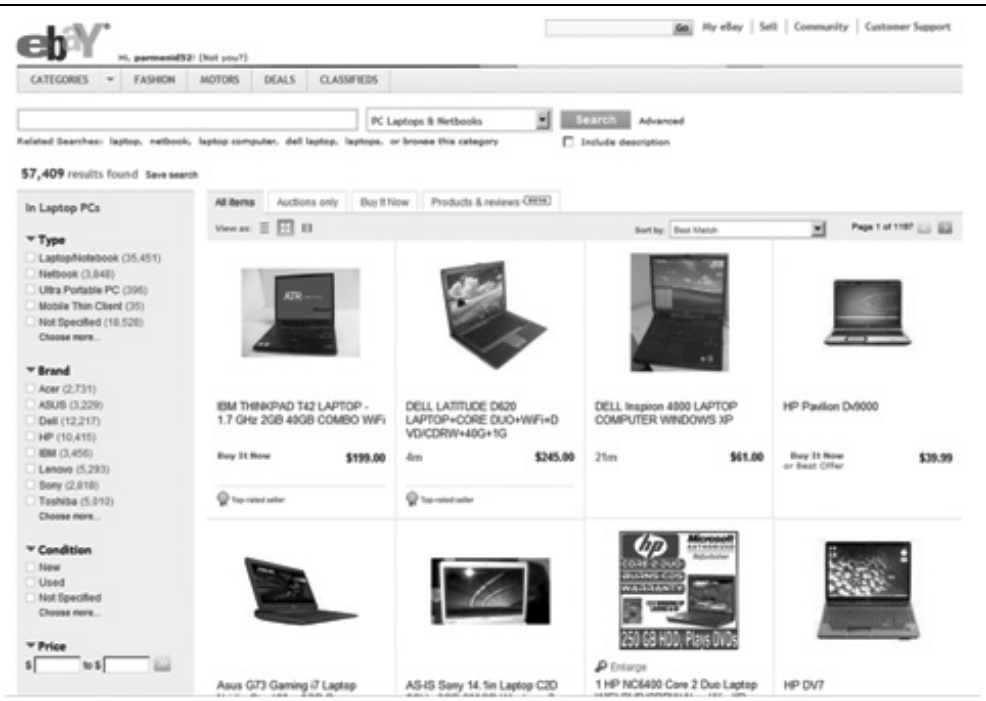
Prijava za kupovinu ili prodaju na eBay-u je jednostavna, brza i besplatna. Dovoljno je popuniti registracionu formu i postaje se član sa pravom nadmetanja u nekoj od mnogobrojnih aukcija koje ovaj sajt nudi, kao i mogućnost da se nešto ponudi na prodaju.



Slika 2.5.2 Registraciona forma za prijavu za rad na eBay-u

Prilikom izbora određenog proizvoda dobijamo niz informacija koje su nam potrebne da bi doneli odluku o kupovini. Pored slike proizvoda najpre se vidi iznos poslednje date ponude. Zatim je tu informacija o tome koliko još dugo je proizvod izložen na aukciji, a onda su dati i troškovi isporuke, kao i destinacije gde se sve vrši isporuka robe. Takođe, kupac može i da vidi istoriju datih ponuda. Nakon uzimanja u obzir svih raspoloživih podataka kupac može doneti odluku o kupovini i klikom na određeno polje da podnese svoju ponudu, Slika 2.5.3.

Finansijski model eBay se zasniva na više komponenti i može se reći da je vrlo kompleksan. Postoje naknade za izlistavanje spiska proizvoda, naknada kada se proizvod proda, plus nekoliko opcionih nakanada koje zavise od različitih faktora. Na primer, eBay u SAD-u naplaćuje $0.20-$80 za izlistavanje spiska proizvoda, i 2-8% na konačnu cenu. eBay poseduje PayPal sistem plaćanja, koji opet ima svoje nakande. eBay takođe zarađuje i od reklama.



Slika 2.5.3 Raspoložive informacije o proizvodu

eBay se ne bavi transportom robe ili novčanim transakcijama između kupaca i prodavaca, osim preko PayPal-a kao svoje pomoćne službe. Prodavac se oslanja na poverenje u kupca da će on izvršiti plaćanje i obrnuto: kupac se oslanja na poverenje da će prodavac zaista isporučiti robu. Da bi podstakao poverenje, eBay javno objavljuje povratne informacije svih učesnika o uspešnosti obavljene transakcije. Na taj način, kupac može da proveri istoriju rada prodavca pre davanja ponude.

Glavni mehanizam zaštite od prevara jeste upravo sistem povratnih informacija od korisnika. Nakon svake obavljene transakcije i kupac i prodavac imaju mogućnost da ocene jedan drugog. Mogu da daju ocene pozitivan, negativan i neutralan i daju kraći komentar. Ovakav sistem povratnih informacija ima i svoje nedostatke:

- I sitne i krupne transakcije nose istu težinu u krajnjem rezultatu;
- Korisnik može ostaviti neistinitu informaciju o radu iz straha od osvete da će i sam biti loše ocenjen;
- Povratna informacija je ograničena na 80 karaktera, pa se može desiti da neko ne može u potpunosti da iskaže svoje primedbe.

Kada korisnik primeti da je bilo kupac bilo prodavac bio neiskren, u slučaju da neko ostavi neistinitu informaciju, spor se može rešiti preko eBay-a. Ako ima previše žalbi na nečiji rad, njegov nalog se automatski gasi.

Neke moguće prevare od strane prodavca su: primanje uplate i neisporuka robe, isporuka robe drugačijeg opisa od naručene, svesno davanje pogrešnog opisa robe, isporuka pogrešne robe, prodaja ukradene robe, „naduvavanje" ponude učestvovanjem na sopstvenoj aukciji preko drugog naloga ili osobe koja radi u interesu prodavca. Neke moguće prevare od strane kupca su: prevara preko PayPal-a (podnošenje neistinitog zahteva za nadoknadu štete) prevara putem kreditne kartice (na primer ukradena kartica), prijem robe a tvrđenje suprotnog, povraćaj robe drugačije od primljene, slanje lažne potvrde o izvršenom plaćanju.

Na samom početku rada, eBay je bio prilično neorganizovan. Kako se širio, tako je sve više jačala potreba da se stvari urede, i da se ograniče ili zabrane aukcije za pojedine vrste proizvoda. Međutim, restrikcije se razlikuju od tržišta do tržišta u zavisnosti od toga kako lokalni zakoni regulišu promet predmetne robe. Među proizvodima koji su zabranjeni spadaju: duvan, alkohol, droga, staro donje rublje i prljava iznošena garderoba, ljudski organi, loto tiketi i drugi.

Trenutna strategija eBay-a je da poveća prihod tako što će uvećati međunarodnu trgovinu kroz eBay sistem. eBay se već proširio na preko dvadeset tržišta, uključujući i Kinu i Indiju. Jedine zemlje gde eBay nije uspeo da se proširi jesu Tajvan, Japan i Hong Kong, gde je Yahoo! vodeći Web sajt ovog tipa.

U toku 2005 godine Ebay-a je utrošio 2,5 milijarde dolara na kupovinu telefonske firme na Internetu „Skype", čime je znatno proširio bazu svojih korisnika na gotovo 480 miliona ljudi. U novembru 2009, ova kompanija je prodata u cilju zadržavanja fokusa na osnovnu delatnost. U 2010 godini kompanija je ostvarila obrt od 9,136 milijardi dolara i neto prihod od 1,801 milijardu dolara. U prvom kvartalu 2008 godine zapošljavala je 15,500 radnika.

2.6 LITERTURA

[1] Ghosh, Shikhar, Making Business Sense of the Internet, *Harvard Business Review,* March-April, 1998

[2] Porter M.E. , V.E.Millar, How Information Gives You Competitive Advantage, *Harvard Business Review,* July-August, 1985

[3] http://en.wikipedia.org/wiki/ List_of_countries_by_number_of_mobile_phones_in_use

[4] http://www.codaresearch.co.uk/

[5] http://www.shop.org

[6] K.C.Laudon, C.G.Traver, *E-Commerce, business, technology, society*, Sixth Ed., Pearson Education Inc., 2010.

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

3. TEHNOLOŠKE OSNOVE ELEKTRONSKE TRGOVINE

U ovom poglavlju se ukratko razmatraju najvažnije računarske i komunikacione tehnologije, koje predstavljaju osnovu celokupne savremene informatičke infrastrukture: Internet i WorldWide Web.

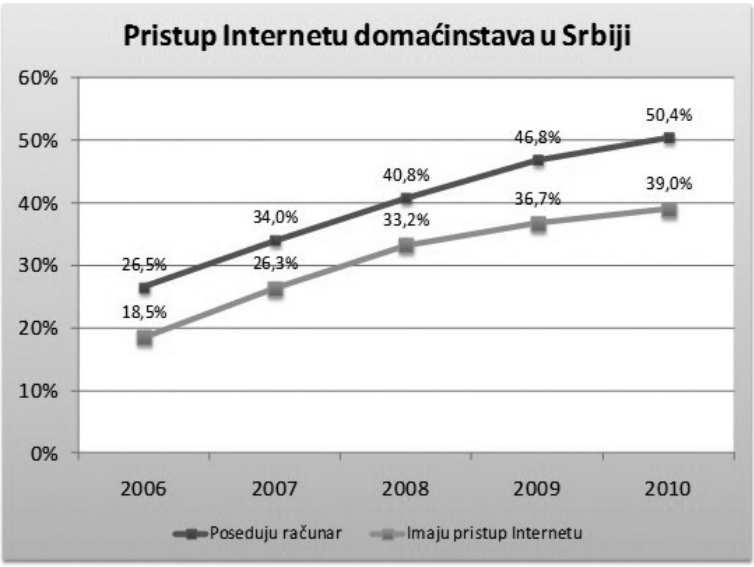
Internet i Web tehnologije nastale su u relativno bliskoj prošlosti i još uvek se veoma brzo razvijaju kroz nove uređaje, tehnologije povezivanja, tehnologije izrade softvera i nove lične i poslovne primene.

3.1. OSNOVE INTERNETA

Računarska mreža je sistem računara povezanih pomoću telefonskih linija ili na neki drugi način radi deljenja informacija [1], [2].

Internet je globalna računarska mreža, koja povezuje veliki broj manjih mreža i pojedinačnih računara u jednu funkcionalnu celinu [1].

Broj povezanih računara ili *host*-ova stalno raste i procenjuje se na više stotina miliona [1],[3], Slika 1.4.1, Slika 3.1. Internet mreža omogućava povezivanje preduzeća, školskih institucija, državnih struktura i pojedinaca radi deljenja resursa, pre svega podataka i softverskih aplikacija, koje se još nazivaju *mrežni servisi*.



Slika 3.1 Opremljenost domaćinstava računarima i pristup Internetu u Srbiji 2006-2010

World Wide Web (u daljem tekstu Web) je deo Interneta dostupan kroz grafički korisnički interfejs, koji se sastoji od dokumenata povezanih hipervezama [4]. Predstavlja jedan od najpopularnijih mrežnih servisa, koji je presudno doprineo širenju upotrebe Interneta.

WorldWide Web se može posmatrati kao globalni grafički hipertekst informacioni sistem, koji se izvršava na Internet mreži. Sadrži posebno formatirane dokumente - Web stranice. Svaka Web stranica (*page*) ima sopstvenu jedinstvenu fizičku adresu u Internet mreži. Fizička adresa stranice se naziva URL adresa (*Uniform Resource Locator*, URL).

Izbor stranice se vrši klikom na hipervezu (*hyperlink*), koja može biti reč, niz reči ili slika u dokumentu. Hiperveza je na grafičkom ekranu posebno označena, npr. podvlačenjem ili drugom bojom.

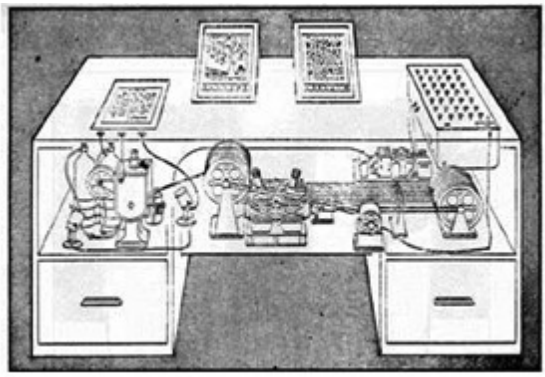
Web dokumenti su formatirani u jeziku HTML (*HyperText Markup Language*). Jezik HTML služi za opis grafičkog izgleda dokumenata, kao i veza s drugim dokumentima. Struktura i prikaz informacija vrši se pomoću više stotina različitih oznaka (*tags*), koje predstavljaju naredbe jezika i njihove atribute.

Jezik HTML je nastao kao kao pojednostavljena verzija složenijeg jezika SGML, ISO standarda za opis vizuelnog (grafičkog) izgleda svih vrsta dokumenta – knjiga, planova, brošura itd. Postoje i drugi jezici namenjeni specifikaciji grafičkog izgleda dokumenta, npr. poznati *PostScript* kompanije *Adobe Systems*, koji se koristi u elektronskom i stonom izdavaštvu.

3.1.1 Nastanak Interneta

Savremena javna Internet mreža nastala je razvojem i komercijalizacijom tehnologije koju je razvila i koristila naučna računarska mreža američkog ministrastva odbrane ARPANET (*Advanced Researches Projects Agency*, ARPA).

Ideju moderne tehnologije povezivanja naučnih informacija izneo je još 1945. godine američki naučnik *dr Vannevar Bush* u članku "As We May Think" za časopis *Atlantic Monthly*, u kome je opisao zamišljeni foto-elektro-mehanički uređaj za pamćenje dokumenata na mikrofišu, koji može da kreira i prati tekstualne veze (*links*) između njih [5], Slika 3.2.



Memex - zamišljeni elektromehanički uređaj (ekran, tastatura, komunikacije) za automatizovano čuvanje i razmenu dokumenata, beleški i komunikacija, koji ima ulogu lične kartoteke i biblioteke.
Ideju je 1945. godine izneo Vannevar Bush, naučnik koji je tridesetih godina 20. veka razvio prvi elektronski analogni računar. Za vreme drugog svetskog rata bio je naučni savetnik američkog predsednika Ruzvelta i osnivač *Office of Scientific Research and Development*, tela koje je nadziralo strategijske projekte, između ostalog i projekt razvoja atomske bombe. Od 1946 do 1947, Bush je predsedavao telu *Joint Research and Development Board*, iz koga se razvila agencija DARPA (*Defense Advanced Researches Projects Agency*), koja će kasnije pokrenuti projekt ARPANET. Vizionarski je opisao buduću upotrebu informacionih tehnologija, što je inspirisalo mnoge kreatore Interneta.

Slika 3.2 - Nastanak ideje moderne tehnologije povezivanja radi razmene informacija

Današnja Internet mreža se intenzivno razvija poslednjih pola veka. U toku njenog razvoja mogu se uočiti tri osnovne faze [1]:

- faza inovacija (1961-1974)
- faza institucionalizacije (1975-1995)
- faza komercijalizacije (1995 do danas)

U *prvoj fazi* su koncipirani i realizovani osnovni hardverski i softverski elementi mrežnog povezivanja: hardver za paketni prenos, klijent-server računarstvo i komunikacioni softverski protokoli, skraćeno nazvani TCP/IP (*Transaction Control Protocol/Internet Protocol*). Početna namena Interneta je bila povezivanje postojećih univerzitetskih računskih centara, koji su do tada mogli samo da razmenjuju fajlove putem telefonskih linija.

Drugu fazu razvoja računarske mreže omogućile su institucije koje su finansirale naučni razvoj u SAD, ministartsvo odbrane (*Department of Defense*, DoD) i nacionalna fondacija za nauku (*National Science Foundation*, NSF), prvo kroz razvoj robusne vojne naučne računarske mreže ARPANET (*Advanced Research Projects Agency Network*), a zatim, od 1986. godine, civilne naučne mreže NSFNet, koja je prerasla u javnu računarsku mrežu nazvanu Internet (skraćeno od *Inter Network*).

Treća faza razvoja traje i danas. U ovoj fazi su državne agencije prepustile dalji razvoj infrastrukture i njenu eksploataciju privatnim kompanijama, što je dovelo do proširenja kruga korisnika mreže i razvoja novih primena u svakodnevnom životu i poslovanju.

Kao datum početka primene Interneta u elektronskoj trgovini uzima se 1994. godina, kada su se pojavili prvi komercijalni oglasi i trgovanje u Internet mreži.

Kratki prikaz značajnih datuma u razvoju Interneta dat je Tabeli 3.1 [1]. Posebno su istaknuti ključni događaji važni za nastanak Interneta, Web-a i elektronske trgovine.

Tabela 3.1 Značajni datumi i faze razvoja Interneta

Godina	Događaj	Značaj
I Faza inovacija		
1961	Objavljen rad o paketnim mrežama (Leonard Kleinrock, MIT)	Nastanak koncepta paketnog prenosa podataka
1961	Povezani računari iz Kembridža i Kalifonije putem sporih linija (Lowrence Roberts, MIT)	Prva demonstracija mreže udaljenih računara (preko 1.000m) povezanih telefonskim linijama (prenos podatka i pokretanje programa, nepouzdano i sporo)
1962	Memorandum o svetskoj mreži računara – Galactic Network (Licklider J.C.R., MIT)	*Vizija globalne računarske mreže*
1963	Na čelu kancelarije ARPA za razvoj tehnika obrade informacija Licklider J.C.R.	Interesovanje vojne Agencije za napredne razvojne projekte (ARPA) za razvoj svetske računarske mreže
1966	ARPA finansira razvoj mreže ARPANET koja se zasniva na komutaciji paketa	Početak razvoja globalne paketne mreže
1968	ARPA traži cene od raznih kompanija radi izgradnje paketne mreže	Koncept komutacije paketa je bliži fizičkoj realizaciji
1969	Prvi uređaji za komutaciju paketa instalirani na UCLA i Stanford University	*Hardverska realizacija koncepta komutacije paketa*

Godina	Događaj	Značaj
1969	Prva paketno-komutirana poruka upućena sa UCLA na Stanford University	Stvoren komunikacioni hardver Interneta (skraćeno od Inter Network)
1972	Pronalazak elektronske pošte i prvog e-mail programa (Ray Tomlinson, kompanija Bolt, Beranek and Newman)	Nastanak prve nezaobilazne aplikacije na Internetu
1973	Pronalazak Ethernet tehnologije i lokalnih računarskih mreža (Xerox PARC laboratorije)	*Nastanak klijent/server računarstva* povezivanjem računara na malim udaljenostima (do 1.000m)
1974	Objavljen rad o "otvorenoj arhitekturi" mrežnog povezivanja i konceptu TCP/IP	*Stvoren koncept TCP/IP protokola*, načina za povezivanje velikog broja različitih lokalnih mreža i računara, kao i jedinstvene šeme adresiranja svih računara u mreži.
II Faza institucionalizacije		
1980	Ministarstvo odbrane SAD usvaja TCP/IP kao standardni komunikacioni protokol	Najveća računarska organizacija na svetu usvaja TCP/IP i komutaciju paketa kao mrežnu tehnologiju
1980	Pronalazak personalnog računara	Pojava stonih računara frrmi *Altair*, *Apple* i *IBM*, koji će milionima ljudi omogućiti pristup Internetu i Webu
1983	Stvara se zasebna vojna mreža (MILNET), dok na ARPANET ostaju samo civilni univerziteti	Nastanak ideje civilnog Interneta
1983	Uvođenje mrežnih servisa Telnet i FTP (*File Transfer Protocol*)	Telnet omogućava udaljenim računarima vezu i pokretanje programa na lokalnim računarima, a FTP lakši prenos fajlova (još dve nezaobilazne aplikacije)
1984	Kompanija Apple uključila program *HyperCard* u grafički orijentisani interfejs OS MacIntosh	Komercijalna upotreba koncepta hiperdokumenta
1986	Nacionalna fondacija za nauku (NSF) usvaja Internet kao svoju interuniverzitetsku mrežu	Počinje program razvoja univerzitetske mreže, koji zahteva od svih univerziteta da koriste sredstva NSF da bi omogućili pristup mreži širom kampusa
1988	NSF ohrabruje razvoj privatnih magistralnih komunikacija radi privatizacije Interneta	Formiranje privatnih kompanija za rukovanje komercijalnim Internet saobraćajem
1989	Predlog razvoja svetske mreže hipedokumenata kreiranih na osnovu jezika nazvanog HTML (Tim Berners Lee, CERN)	*Nastanak nove Internet usluge nazvane World Wide Web*
1990	NSF preuzima odgovornost za infrastrukturu civilnog Interneta, kreira NSFNet i zatvara APANET	Koncept civilnog Interneta otvorenog za sve se realizuje se finansijsku podršku NSF

Godina	Događaj	Značaj
1990	Raste osnova Interneta (backbone)	Od početnih 6 čvorova brzine 56kbps 1990. godine osnova Interneta narasta na 21 čvor brzine 45Mbps, koji povezuju 50.000 mreža na svim kontinetima
1993	Nastao *Mosaic*, prvi grafički orijentisan Web čitač (Mark Andreesen; verzija za Macintosh Aleksandar Totić; NCSA, Univ. of Illionois)	Veoma pojednostavljena upotreba Web dokumenata za obične korisnike
1994	NSF objavljuje planove razvoja informatičke supermagistrale za podršku univerziteta, poslovanja i građana	Kongres i kancelarija predsednika SAD predlažu kreiranje nacionalne informatičke infrastrukture za podršku istraživanja, edukacije, trgovine i lične potrebe
1994	Osnovana kompanija Netscape Corporation (Mark Andreesen i Jim Clark)	Prvi komercijalni Web čitač
1994	Prvi komercijalni oglasi (*banner*) na sajtu Hotwired.com	*Početak e-trgovine (I era)*
III Faza komercijalizacije		
1995	NSF privatizuje osnovu interneta	Potpuno komercijalizovan civilni Internet - formirana i privatna kompanija za dodelu Internet adresa
1996	Osnovan konzorcijum Internet2	Državne agencije, univerziteti i kompanije planira razvoj 100-1.000 puta bržeg Interneta
1998	Vlada SAD pospešuje osnivanje korporacije za dodelu Internet imena i adresa ICANN	Upravljanje imenima domena i adresama se prenosi na privatnu neprofitnu međunarodnu organizaciju
2002	Ministarstvo trgovine SAD produžava svoj ugovor sa ICANN do 2003.	Porast zahteva za više državne intervencije u upravljanju Internetom i kritika ICANN, čija se uloga privremeno produžava
2003	Brza Internet2 mreža *Abilene* dostiže brzinu 10Gbps; u Intnternet2 mreži 200 univerziteta, 60 poslovnih i 40 ostalih organizacija	Ostvaren značajan napredak u razvoju višestruko brže interkontinentalne osnove Interneta
2005	NSF predlaže inicijativu za razvoj novih osnovnih funkcija Interneta, poboljšanu arhitekturu zaštite, visoku raspoloživost i nove servise i aplikacije (*Global Environment for Networking Investigations*, GEN)	Uočeno da buduća Internet zaštita i funkcionalne potrebe mogu zahtevati temeljno preispitivanje postojeće tehnologije

Prva zvanična definicija Interneta formulisana je 1995. godine u rezoluciji *Federal Networking Council* (FNC), tela zaduženog za Internet. U posebnoj rezoluciji, pojam 'Internet' je definisan kao *globalni informacioni system, koji je (i) logički povezan u celinu pomoću jedinstvenog globalnog adresnog prostora zasnovanog na Internet protokolu (IP) ili njegovim proširenjima ili sledbenicima; (ii) u stanju je da podrži komunikacije koristeći*

skup protokola Transmission Control Protocol/Internet Protocol (TCP/IP) ili njegovim narednim proširenjima ili sledbenicima i/ili drugim protokolima kompatibilnim sa IP; (iii) obezbeđuje, koristi ili čini dostupnim, bilo javno ili privatno, usluge visokog nivoa po slojevima komunikacija i u vezi sa opisanom infrastrukturom [1].

Tako je savezna komisija za umrežavanje SAD definisala Internet kao računarsku mrežu koja:

- koristi IP adresiranje
- podržava skup protokola nazvan TCP/IP
- pruža usluge korisnicima, na sličan način kao telefonski sistemi.

3.1.2 Najvažnije tehnologije na kojima se zasniva Internet

Suština zvanične definicije Interneta je isticanje tri važna tehnološka koncepta, koja predstavljaju osnovu za razumevanje Interneta:

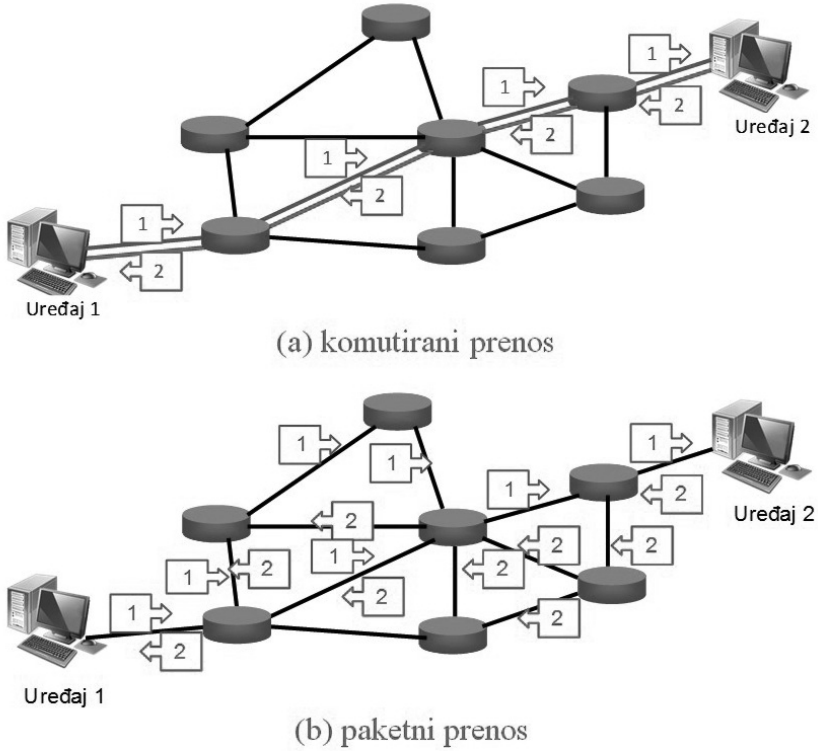
- prenos podataka komutacijom paketa
- skup komunikacionih protokola TCP/IP
- klijent/server računarstvo

Paketni prenos

Prenos digitalnih podataka između dva računara u klasičnim komutacionim (prespojnim) mrežama podrazumeva uspostavljanje neprekidne veze između njih i njeno zauzeće sve vreme trajanja prenosa podataka. Pri tome se prespajanje ne vrši samo na jednom mestu, već u tome učestvuje veći broj komutacionih uređaja (čvorova, centrala). Ukoliko se prenosi velika količina poodataka, zauzeće svih čvorova i spojnih puteva može da potraje dugo, pri čemu drugi zahtevi čekaju da se veza oslobodi. Osim toga i to vreme se ne troši racionalno, jer se npr. u telefonskim razgovorima i do 2/3 vremena ne prenosi govor, već se raspoloživo vreme troši na pauze između izgovorenih reči i kašnjenje zbog povezivanja delova komutacionog sistema.

Jedno rešenje ovog problema je paketni prenos podataka. Digitalni podaci se dele na male segmente, tzv. pakete (*packets*), označi se njihovo odredište, tako da se od pošiljaoca do odredišta mogu slati različitim putevima. Na odredištu se prikupljaju i sastavljaju u celinu.

Na ovaj način se propusnost mreže povećava za više redova veličina, jer se istovremeno prenosi mnogo veći broj poruka (naravno, po delovima) i kapacitet prenosa se maksimalno koristi. Pri tome se samo vreme prenosa pojedinačne poruke produžava, jer se prenosni put deli, radi prenosa delova drugih poruka. Na slici 3.2 je ilustracija dva načina prenosa poruka između računara u mreži.



Slika 3.3 Komutirani i paketni prenos podataka

Brzina prenos podataka se meri brojem prenesenih bita u jedinici vremena, npr. za broj prenesenih bita u sekundi koristi se oznaka *bps* (*bits per second*, bit se označava malim slovom, a 8-bitni bajt velikim).

Na slici 3.4 je neformalna ilustracija paketnog prenosa digitalnih podataka. Digitalni zapis poruke se deli na pakete fiksne dužine, načelno oko 1.5KB. Paketima se dodaje zaglavlje, koje sadrži adrese pošiljaoca i primaoca, dužinu cele poruke i ukupan broj paketa koji čine poruku i koje primalac treba da primi.

Tekst poruke ...	originalni tekst poruke
00101101100010011011100011101	digitalizovani tekst (niz bita)
01100010 10101100 11000011	podela niza bita na *pakete* (tipično oko 1500 bajtova)
0011001 10101100 11000011	dodavanje zaglavlja svakom *paketu* (adresa odredišta, dužina paketa, broj paketa u poruci, itd.)

Slika 3.4 Ilustracija paketnog prenosa podataka

Prijemni računar mora da potvrdi (*aknowledgement*) prijem svakog paketa, tako da veliki deo vremena računarska mreža prenosi samo poruke potvrde o prijemu paketa. One su uzrok dodatnog kašnjenja paketa, koje se naziva latencija (*latency*).

Posrednici u prenosu paketa kroz paketnu računarsku mrežu su računari posebne nemene, koji se zovu ruteri (*routers*). Njihov zadatak je da prihvate pakete koji su im upućeni i proslede ih najpogodnijim putem prema odredišnom računaru. Upravljački programi koji biraju najpogodniji raspoloživi put paketa nazivaju se programi/algoritmi rutiranja (*routing algorithms*).

Važna posledica postupka rutiranja je svojstvo paketnih mreža da, ako dođe do preopterećenja ili prekida u radu nekog dela mreže, automatski preusmere saobraćaj na drugi raspoloživi pravac.

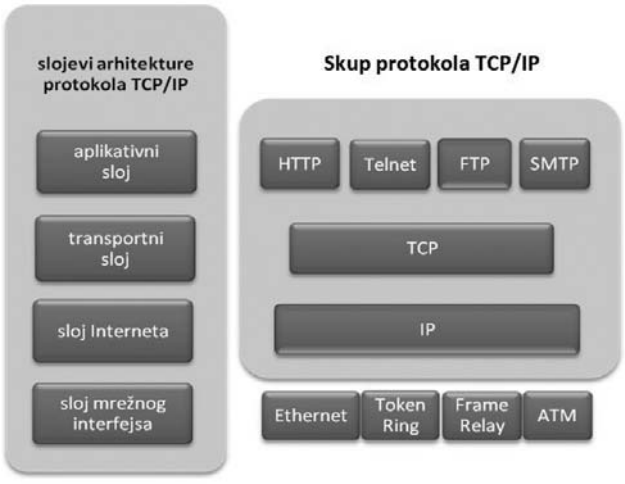
Skup protokola TCP/IP

Standardizacija komunikacija za paketni prenos podataka dovela je do skupa pravila (protokola) koja definišu metode podele poruke na pakete, njihovog rutiranja i sastavljanja izvorne poruke na odredištu.

Skup protokola za paketni prenos podataka nazvan je *Transmission Control Protocol/ Internet Protocol*, skraćeno TCP/IP. Protokol je skup pravila za formatiranje, određivanje redosleda, optimizaciju kodiranja (kompresiju), proveru ispravnosti poruka i druga pitanja slanja i prijema poruka u mreži.

Protokol TCP/IP uspostavlja vezu između računara pošiljaoca i primaoca poruke i rukuje podelom poruke na pakete, te njenim sastavljanjem na prijemnoj strani. Internet protokol obezbeđuje adresnu šemu Interneta.

Realizacija ovih protokola može biti hardverska ili softverska, a razmatra se na više različitih nivoa posmatranja mrežne komunikacije, tzv. slojeva (*network layers*), Sl. 3.5. Sloj mrežnog interfejsa obezbeđuje vezu i prilagođavanje različitih lokalnih mreža (kao što je Ethernet), sloj Internet mreže paketni prenos, adresiranje i rutiranje, transportni sloj obezbeđuje komunikaciju s aplikacijom, a aplikativni sloj obezbeđuje aplikacije koje pristupaju uslugama nižih slojeva, kao što su *HyperText Transfer Protocol* (HTTP), *File transfer Protocol* (FTP) i *Simple Mail Transfer Protokol* (SMTP).



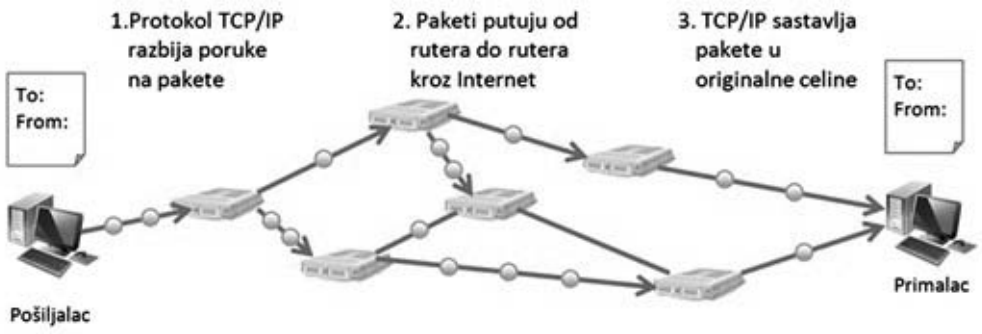
Slika 3.5 Višeslojna arhitektura skupa mrežnih protokola TCP/IP

Standardna Internet adresa je 32-bitni niz bita, koji se obično preglednije predstavlja pomoću četiri osmobitne komponente, koje se pišu u decimalnom obliku, razdvojeni tačkom, npr. 192.168.60.10 (vrednost pojedinačnog bajta može biti 0-255 decimalno). Prve tri cifre su namenjene adresiranju lokalnih mreža, dok poslednja predstavlja adresu pojedinačnog računara u jednoj lokalnoj mreži.

Ovakva 32-bitna adresa se koristi u standardnoj verziji Internet protokola (verzija 4, skraćeno IPv4), koja je još uvek u upotrebi, obezbeđuje 2^{32} adresa, odnosno nešto više od 4 milijarde adresa za sve računare u svetskoj mreži.

Ovo je nedovoljno, posebno nakon brzog rasta broja korisnika mobilnih komunikacija (u svetu je registrovano preko 5 milijardi korisnika mobilnih telefona [6]) i razvoja bežičnog Interneta. Zbog toga se za nove primene uvodi novija verzija Internet protokola (verzija 6, skraćeno IPv6), koja ima 128-bitnu adresu i obezbeđuje 2^{128} različitih adresa (oko $3{,}4 \times 10^{38}$), što je veoma velika vrednost, npr. znatno više od broja zvezda u poznatom svemiru (*observable universe*), koji se procenjuje na 10^{24} [6].

Na Sl. 3.6 je pojednostavljen prikaz procesa rutiranja poruka u paketnoj mreži, koja se zasniva na skupu protokola TCP/IP [1].



Sl. 3.6 Rutiranjem Internet poruka u paketnoj TCP/IP mreži

Duge numeričke Internet adrese nisu praktične za upotrebu od strane ljudi. Zbog toga se za komunikaciju u prirodnom jeziku koriste njihove tekstualne zamene, koje se formiraju u skladu s konvencijom o nazivima domena.

Sistem naziva domena (*Domain Name Sistem*, DNS) omogućava zamenu IP adresa njihovim tekstualnim ekvivalentima, npr naziv *cnet.com* predstavlja IP adresu 216.200.247.134. Na taj način Web čitači mogu da pronalaze tražene Web sadržaje.

Tekstualni nazivi adresa nazivaju se još URL adrese (od *Uniform Resource Locator*, URL). Opšta forma URL adrese je:

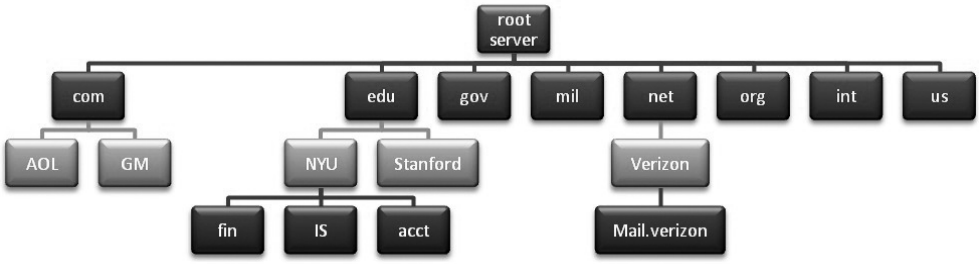
protokol://ime_servera.ime_domena/folder_resursa/resurs

- *protokol* je skup pravila za komunikaciju klijenta i servera (*http*, *https*, *ftp*, i sl.)
- *ime_servera* je oznaka servera koji prima poruku; uz protokol *http*, oznaka Web servera *www* se može izostaviti, jer je Web čitači podrazumevaju
- *folder_resursa* je naziv foldera na serverskom računaru
- *resurs* je naziv objekta na folderu servera; ako se ne navede, Web serveri koriste neki zadani podrazumevani naziv, npr. *index.html* ili *default.htm*

Primer URL adrese je *http://www.wikipedia.org/flash_test*, koja se odnosi na IP adresu 208.80.152.2. Naziv domena je "wikipedia.org", protokol za pristup adresi je *Hypertext Transfer Protocol* (HTTP). Sam resurs pod nazivom "flash_test" nalazi se na serveru, na putanji */flash_test*.

Naziv domena u URL adresi može da ima od dva do četiri dela, npr. *cnet.com* ili *dls.singidunum.ac.rs*.

Na Slici 3.7 je prikaz dela osnovne strukture sistema naziva Internet domena (DNS). Sistem imena domena uređen je hijerarhijski i služi za imenovanje svih Internet resursa. Posebni korenski (*root*) serveri realizuju prvi korak prevođenja tekstualne Internet adrese u numeričku, koja se dalje koristi u računarskoj komunikaciji. Od 2009. godine, korenski domen ima 20 osnovnih i 248 imena nacionalnih domena (nacionalni domen Republike Srbije je *rs*) [6].



Slika 3.7 Osnovna struktura sistema naziva Internet domena

Komponente šeme adresiranja na Internetu su IP adrese, nazivi domena (*Domain Names*) i DNS serveri.

IP adresa ili adresa Internet protokola (IP) je jedinstvena numerička adresa svakog računara koji je stalno povezan u Internet mrežu. Računari koji se povezuju pomoću modema dobijaju privremene IP adrese.

Nazivi domena su tekstualni ekvivalenti numeričkih IP adresa, koje ljudi lakše koriste. Sistem koji omogućava predstavljanje numeričkih IP adresa pomoću tekstualnih izraza naziva se sistem naziva domena ili skraćeno DNS (*Domain Name Sistem*).

DNS serveri su baze podataka koje prate IP adrese i imena domena na Internetu. Korenski ili *root* serveri su centralni folderi, sa spiskom svih naziva domena koji su trenutno u upotrebi za određene domene, npr. *root* server za domen *.com*. DNS serveri konsultuju korenske servere za pronalaženje nepoznatih imena domena prilikom rutiranja saobraćaja.

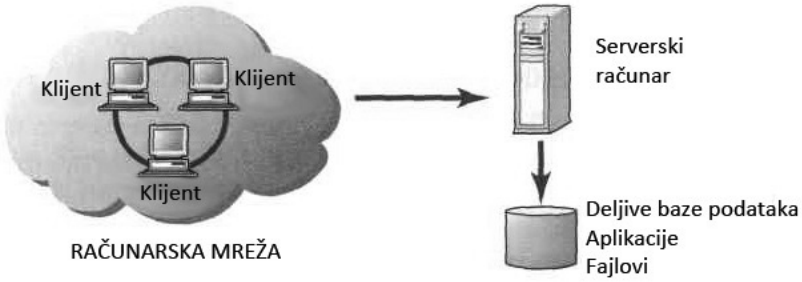
Internet korporacija za dodelu brojeva i imena (*Internet Coporation for Assigned Numbers and Names*, ICANN) osnovana je 1998. godine, radi uspostavljanja pravila za imena domena i IP adrese, kao i za koordinaciju rada korenskih servera, što su do tada vršile privatne firme.

3.1.3 Internet protokoli i uslužni programi

Uspostavljanje mrežnih standarda u paketnim računarskim mrežama i naglo povećanje njihovog kapaciteta prouzrokovalo je značajne promene u računarstvu, koje su dovele do razvoja današnjeg Interneta i Web-a.

Ključna promena je u modelu upotrebe računara, koji je dobio naziv klijent/server model, odnosno klijent-server računarstvo (*Client/Server Computing*). Celokupna javna Internet mreža je primer primene tog modela, u kome stotine miliona klijetskih računara ima pristup milionima Web servera širom planete.

Klijent/server računarstvo je model računarske mreže povezanih snažnih ličnih računara (klijenti) i jednog ili više serverskih računara, slika 3.8 [1].



Slika 3.8 Model klijent-server računarstva

Klijenti mogu biti stoni ili ručni lični računari, koji mogu samostalno da izvršavaju veoma složene zadatke, kao što je npr. prikaz zahtevne grafike, obrada slike i zvuka i čuvanje velikih fajlova.

Serveri su računari povezani u računarsku mrežu, koji izvršavaju zajedničke funkcije, koje su potrebne klijentskim računarima, kao što je npr. skladištenje podataka, izvršavanje određenih aplikacija, mrežno povezivanje i štampanje.

Moderni personalni računari se mogu koristiti istovremeno kao klijenti i kao serveri u distribuiranoj računarskoj mreži bez centralnog upravljanja (*peer-to-peer* računarstvo).

Mrežno računarstvo (*Cloud Computing*) je nova forma računarstva nezavisnog od lokacije upotrebljenih računarskih resursa (računara, programa i podataka), slično korišćenju resursa iz javne električne mreže. Naziv je nastao od grafičkog simbola oblaka, kojim se često u dijagramima prikazuje Internet i telekomunikaciona mreža.

Internet protokoli i uslužni programi

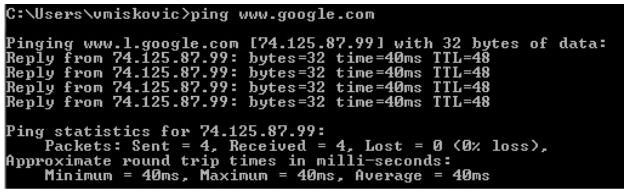
Internet serveri i klijenti koriste Internet protokole kao mrežne aplikacije, koje predstavljaju javno vlasništvo:

- Protokol HTTP (*HyperText Transfer Protocol*) se koristi za prenos stranica između dva računara. Sesiju pokreće klijent slanjem zahteva za resursom (HTTP request). Server odgovara slanjem traženog resursa (npr. Web stranice) i okončava sesiju.
- Protokoli za slanje pošte serveru SMTP (*Simple Mail Transfer Protocol*) i za pregled i preuzimanje pošte sa servera POP (*Post Office Protocol*) predstavljaju standarde za slanje i prijem elektronske pošte. Nešto savremeniji protokol IMAP (*Internet Message Access Protocol*) omogućava pretraživanje, organizovanje i filtriranje pošte pre preuzimanja, na samom serveru elektronske pošte.
- Protokol FTP (*File Transfer Protocol*) je efiksan namenski Internet servis za prenos programa i čitavih baza podaka jednim zahtevom. Koristi se za prenos velikih fajlova, većih od Web stranica i poruka elektronske pošte.
- Protokol aplikativnog sloja *Telnet* koristi se za prijavu klijentskog računara na udaljeni računar putem računarske mreže, radi pokretanja programa ili pristupa fajlovima sa udaljene lokacije.
- Poseban protokol za zaštitu podataka koji se prenose između klijenta i servera je SSL (*Secure Socket Layer*), koji šifruje i digitalno potpisuje sadržaj poruka.

Korisni programi za ispitivanje mreže

Svi mrežni operativni sistemi raspolažu korisnim programima za administraciju i prikupljanje nekih osnovnih informacija o stanju računarskih mreža. Najpoznatiji programi u operativnim sistemima Windows, Unix i Linux su *ping*, *tracert* i *pathping*. Koriste se kao komade operativnog sistema, pa su za njihovo korišćenje potrebna administratorska ovlašćenja.

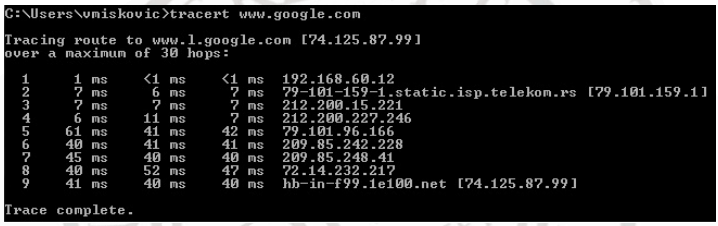
Program *ping* služi za testiranje dostupnosti nekog računara u Internet mreži i merenje vremena putovanja paketa od polaznog do ciljnog računara. Meri se vreme od trenutka slanja posebne testne poruke do potvrde o njenom prijemu, a beleže se i eventualni gubici paketa. Standardno se šalju četiri testne poruke, za koje se dobijaju statistički obrađeni podaci kao na Slici 3.9.



Slika 3.9 Primer izvršavanja programa *ping*

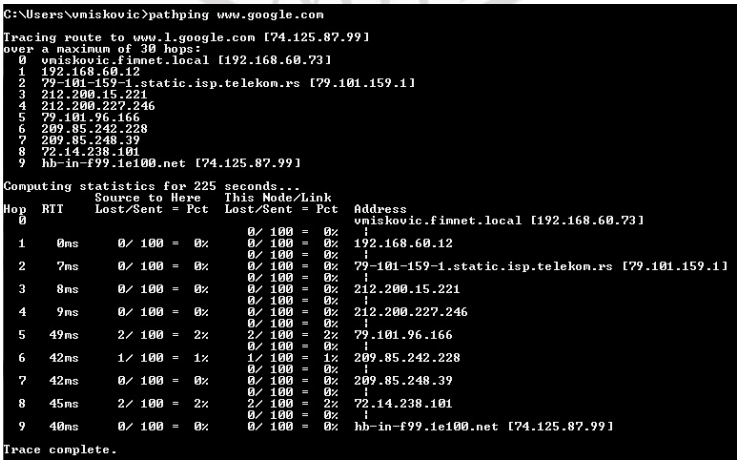
Ovaj program se može i zloupotrebiti, ako se koristi tako da optereti Internet mrežu i ciljni računar testnim paketima, što je tipični napad tipa DOS (*denial-of-service*).

Program *tracert* služi za prikupljanje podataka o putanji i trajanju putovanja paketa kroz paketnu mrežu u operativnom sistemu Windows (u operatvnom sistemu *Linux*, program se zove *tracepath*). Program prikazuje spisak računara preko kojih su paketi prošli na putu do svog odredišta, kao i vreme zadržavanja na svakom od njih, Slika 3.10.



Slika 3.10 Primer izvršavanja programa *tracert*

Funkcije programa *ping* i *tracert* objedinjava program za praćenje mrežne trase paketa *pathping*, koji je uveden u novije verzije operativnog sistema Windows. U operativnom sistemu *Unix*, odgovarajuća komanda ima naziv *mtr* (skraćeno od *my traceroute*).



Slika 3.11 Primer izvršavanja programa *pathping*

Program vraća informacije o detaljima putanje između dva mrežna računara i statistiku vremena putovanja paketa do svakog od njih, koja se prikuplja određeno vreme, Slika 3.11.

3.2. SAVREMENA INTERNET MREŽA

Infrastruktura Internet mreže danas omogućava povezivanje gotovo dve milijarde korisnika širom sveta ([8], jun 2010). Zahvaljujući klijent-server modelu i višeslojnoj arhitekturi, moguća su i dalja proširenja radi povećanja kapaciteta i performansi mreže.

3.2.1 Sadašnja struktura Interneta

Savremena Internet mreža se sastoji od osnove ili kičme meže (*backbone*), koja se sastoji od mreža koje su vlasništvo velikih provajdera Internet usluga (*Network Service Provider*, NSP). Za povezivanje se koriste optička vlakna da bi se postigle velike brzine prenosa od 155Mbps do 2,5/10GBps. Interkontinentalne veze su ostvarene podmorskim optičkim kablovima i satelitskim vezama, a visoka pouzdanost osnove obezbeđuje se visokom redundansom mrežnih uređaja i spojnih puteva.

Pristup osnovi Interneta se ostvaruje preko posebnih priključnih mesta (*Network Access Point*, NAP), koja se još nazivaju i regionalna mesta razmene (*Metropolitan Area Exchange*, MAN), Slika 3.12.

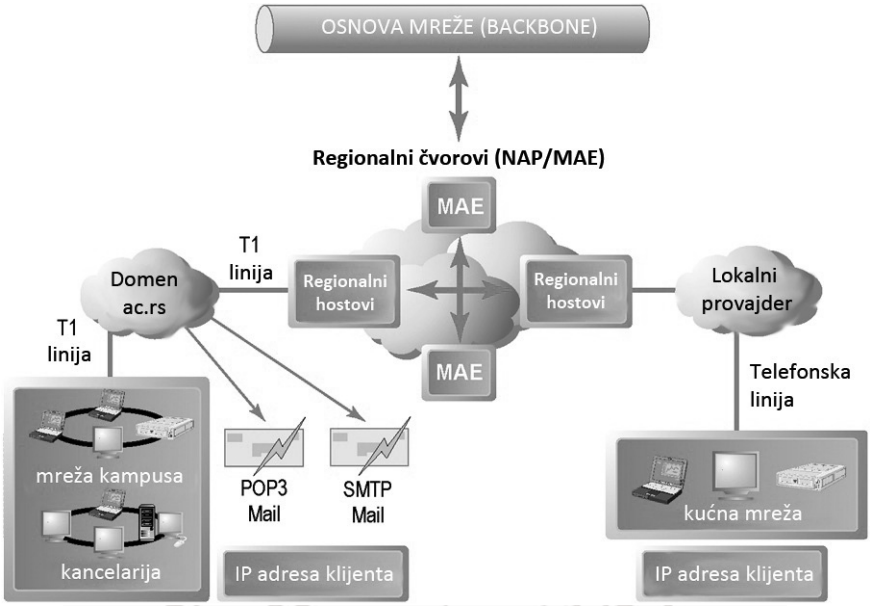
INTERNET II I E-TRGOVINA: DODATNE OPCIJE I USLUGE

IP Telefonija je opšti izraz za tehnologiju koja koristi Internet, kao mrežu sa komutacijom paketa, u cilju prenosa govora i VOIP (*Voice Over Internet Protocol*), protokola preko kojeg se prenosi govor i drugi vidovi audio komunikacije preko Internet protokola.

Digitalne biblioteke - distribucija aplikativnog softvera, multimedije i drugih usluga na bazi plaćanja preko Application Service Providers (ASP)

Distribuirana memorija - ASP može da asistira i u prenosu i u memorisanju podataka, raspodeljujući ih različitim, a ne samo jednom serveru

Mreže kampusa su računarske mreže organizacija, direktno spojene na regionalnu infrastrukturu, koje mogu da objedinjavaju veliki broj lokalnih mreža unutar organizacije.



Slika 3.12 Arhitektura Internet mreže

Lokalni provajderi ili davaoci Internet usluga (*Internet Service Providers*) bave se maloprodajom Internet usluga direktno pojedincima i manjim organizacijama. Brzina komunikacija provajdera prema regionalnom nivou je obično 45Mbps-155Mbps, a brzina povezivanja na Internet krajnjih korisnika trenutno je do 16Mbps.

Internet tehnologije se u organizacijama koriste na dva načina, kao *intranet* (interna računarska mreža zasnovana na Internet tehnlogijama) i *extranet* (deo računarske mreže organizacije dostupan korisnicima izvan same organizacije).

Upravljanje Internet mrežom

Pošto ne postoji jedan vlasnik infrastrukture ili tehnologije Interneta, kao ni institucija koja upravlja celokupnom mrežom, na rad svetske javne mreže utiču i vrše nadzor međunarodna regulaciona tela, nacionalna zakonodavstva i međunarodna profesionalna udruženja.

Najpoznatije institucije koje utiču na funkcionisanje i razvoj Interneta su:

- *Internet Architecture Board* (IAB) pomaže u definisanju sveukupne strukture Interneta.
- *Internet Corporation for Assigned Names and Numbers* (ICANN) dodeljuje IP adrese i nazive Internet domena.
- *Internet Engineering Steering Group* (IESG) nadgleda donošenje Internet standarda.

- *Internet Engineering Task Force* (IETF) predviđa naredne korake razvoja Interneta i nadgleda njegov rad i razvoj.
- *Internet Society* (ISOC) je konzorcijum korporacija, državnih agencija i neprofitnih organizacija, koje nadziru pravila i praksu upotrebe Interneta.
- *World Wide Web Consortium* (W3C) postavlja programske standarde za Web.
- *International Telecommunications Union* (ITU) telo koje pomaže u uspostavljanju tehničkih standarda.

3.3. INFRASTRUKTURA BUDUĆEG INTERNETA

Opšti tehnološki razvoj utiče i na razvoj javne računarske mreže. Infrastruktura buduće mreže se često naziva Internet2 [1].

Veliki deo infrastrukture postojeće Internet mreže je star više decenija, što prouzrokuje probleme i brojna ograničenja u njenom funkcionisanju:

- Ograničenu i nedovoljnu propusnost (*bandwith*) osnove Interneta, prespojnih mesta i lokalnih veza, koji su posebno važni za lične primene i mala preduzeća. Pojava zagušenja u mreži naročito otežava prenos videa i govora.
- Ograničen kvalitet usluge (*quality of service*), koji nastaje zbog pojave kašnjenja paketa (*latency*). Postojeća mreža ne garantuje isporuku paketa (nivo usluge *best effort*) niti razlikuje vrstu saobraćaja.
- Ograničenja arhitekture prouzrokuju zagušenja mreže usled multiplikacije prometa kod preuzimaja različitih multimedijskih sadržaja
- Jezik HTML pruža ograničenu podršku prilikom razvoja i razmene dinamičkih i složenih dokumenata, kao što su baze podataka, poslovni dokumenti i složena grafika.
- Kablovska priroda Interneta ograničava mogućnost širenja mreže i pokretljivost korisnika.

Zbog toga se pristupilo razvoju i uvođenju sledeće generacije Internet tehnologija, koja se često naziva Internet II.

3.3.1 Internet II

Jedan od aspekata razvoja budućeg Interneta II je Internet2®, konzorcijum više od 200 univerziteta, vladinih agencija i privatnih preduzeća, koji sarađuju u cilju iznalaženja načina za što efikasnije korišćenje Interneta.

Projekt se sastoji u izradi velike probne računarske mreže, koja neće remetiti rad postojeće. Najvažniji ciljevi su kreiranje najmodernije računarske mreže za potrebe nacionalnih istraživačkih krugova, omogućavanje revolucionarnih primena Interneta i obezbeđenje pristupa mrežnim servisima i aplikacijama širem krugu korisnika.

Napredna mrežna infrastruktura je dobila naziv *gigaPop* (*gigabit Point of Presence*), u kojoj se na pristupnim tačkama obezbeđuje minimalna brzina prenosa od 1Gbps.

U okviru projekta se ispituju i usvajaju nove mogućnosti, koje obuhvataju:

- razvoj i uvođenje najsavremenijih primena, koje ne postoje u sadašnjoj mreži;
- razvoj i implementacija novih usluga, kao što su *multicast* prenos, protokol IPv6 i bezbednost, koji nisu mogući u postojećoj mreži;
- povezivanje razvojnih i obrazovnih institucija na svetskom nivou, radi razvoja novih načina saradnje;
- pristup istraživačima podacima o radu eksperimentalne mreže i novih aplikacija;
- kreiranje mrežne infrastrukture za komunikacije tipa jedan–prema–mnogima (*multicast*).

Novi Internet predviđa standardizaciju tzv. srednjeg aplikativnog sloja (*middleware*), koji uključuje identifikaciju, autentifikaciju, autorizaciju, direktorijumske i bezbednosne servise. Jedan od rezultata je mogućnost videokonferencija visoke rezolucije (formata ekrana), sa veoma velikim brojem učesnika.

Razvijaju se mnoge napredne primene, kao što su distribuirano računarstvo, virtuelne laboratorije, digitalne biblioteke, distribuirano učenje i sinteza svih ovih mogućnosti u jedinstveno radno okruženje.

Osim ovog projekta, pokrenuti su i drugi razvojni projekti, kao što je inicijativa GENI Nacionalne fondacije za nauku (NSF) i značajne privatne inicijative za dalji razvoj optičkih i bežičnih komunikacija.

Optički kablovi omogućavaju zamenu klasičnih telekomunikacija u osnovi Interneta novim vezama velike brzine, kao i osavremenjavanje starijih optičkih komunikacija novim tehnološkim rešenjima, koja se zasnivaju na dostignućima *fotonike* (proučava komunikacije pomoću svetlosti).

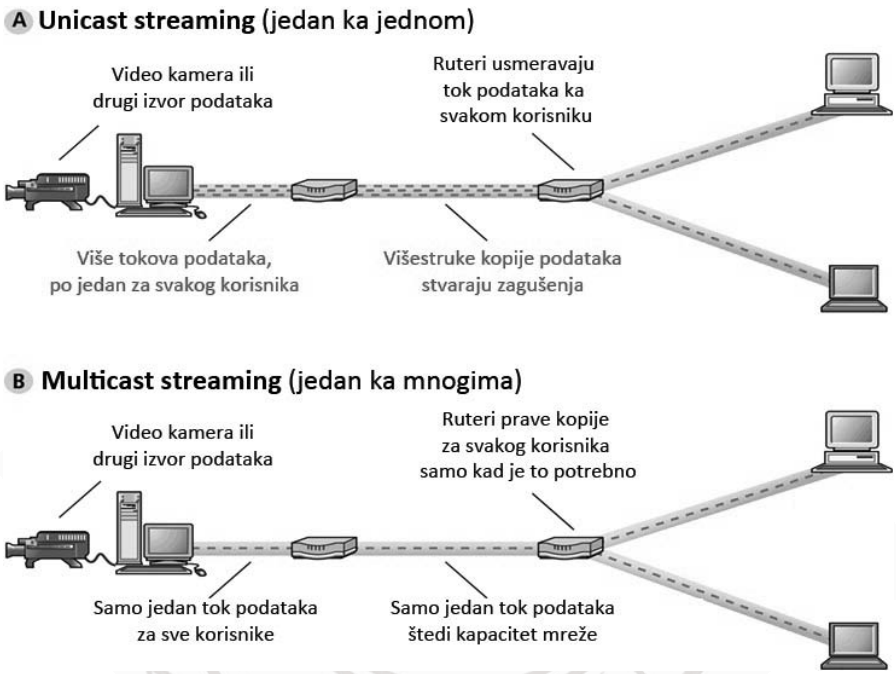
Osim povećanja brzine osnova Interneta (tzv. "prvi kilometar") i regionalnih veza (fiksih ili bežičnih, kao *Wi-Max*), zbog velikih zahteva nekih važnih primena, kao što je prenos govora i videa visoke rezolucije, potrebno je povećati brzinu komunikacije i do svakog korisnika (tzv. "poslednji kilometar").

Povećanje brzine se postiže unapređenjem lokalnih kablovskih mreža i bežičnih komunikacija (*Bluetooth*, *Wi-Fi* i *ZigBee*) namenjenih mobilnim uređajima, kao što su ručni računari, moderni mobilni telefoni i daljinski upravljani uređaji.

Prednosti Internet II tehnologije

Prednosti tehnologije Interneta II obihvataju:

- Efikasan prenos podataka ili *IP multicasting*, niz tehnologija koje omogućavaju efikasnu isporuku podataka na mnoge adrese u mreži, Slika 3.13 [1];



Slika 3.13 Ilustracija istovremenog slanja sadržaja na više adresa (*multicasting*)

- Rešenje problema kašnjenja (*latency*), tako što se vrši klasifikacija paketa po prioritetu i vrsti podataka koje prenose (*differentiated quality of service*);
- Garantovanje nivoa usluge, odnosno mogućnost nabavke prava da se podaci prenose kroz mrežu garantovanom brzinom u zamenu za višu cenu;
- Smanjenje nivoa grešaka i poboljšanje kvaliteta prenosa, usled povećanja kapaciteta i poboljšanja komutacije paketa;
- Smanjenje troškova – veći broj korisnika snižava troškove po jednom korisniku.

3.4. WORLD WIDE WEB

3.4.1 Princip funkcionisanja World Wide Web-a

WorldWideWeb (*WWW*, *W3* ili samo *Web*) je sistem Internet servera koji podržava posebno formatirane dokumente [1]. Dokumenti su formatirani u posebnom jeziku pod nazivom HTML (*HyperText Markup Language*), koji omogućava veze prema drugim dokumentima, kao i grafičkim, audio i video fajlovima.

Hipertekst

Termine *HyperText* i *HyperMedia* uveo je Ted Nelson u svom članku iz 1965. godine [7]. Zamislio je projekat svetskog sistema za elektronske publikacije koji bi predstavljao neku vrstu univerzalne svetske biblioteke. Hipertekst (*HyperText*) je tekst koji ne mora da bude linearan, odnosno tekst koji sadrži veze prema drugim tekstovima. Termin *HyperMedia* se koristi za hipertekst koji ne mora da bude samo običan tekst, već može da sadrži druge multimedijske sadržaje, npr. grafiku, video i zvuk.

Za hipermedijske dokumente važe dva osnovna principa:

1. Svaka stranica dokumenta (*page*) ima sopstvenu fizičku adresu (u slučaju *World-Wide Web*-a, njegov *Uniform Resource Locator* ili URL).
2. Čitalac se može pomeriti sa jedne stranice na drugu pokazivanjem (npr. klikom miša) na reč, niz reči ili sliku, koji predstavljaju vezu (*link*). Veza je dizajnirana i posebno označena na ekranu, npr. osvetljena u drugoj boji ili potcrtana.

Klikom miša na takvu vezu, prelazi se na stranicu čija se adresa kod većine Web čitača prikazuje na dnu aktivnog prozora kada se preko nje prelazi uz pomoć miša.

Svaka stranica može da ima relativno mnogo veza sa drugim stranicama. Čitalac može da izabere jednu od njih ili da ručno unese sasvim proizvoljnu drugu adresu.

Tehnički, Web predstavlja globalni grafički *HyperText* informacioni sistem koji se izvršava na Internet mreži. Predstavlja samo deo Interneta, koji se sastoji od različitih vrsta servera, koji nisu deo *Web*-a.

Pristup dokumentima se ostvaruje preko posebnih aplikacija, tzv. *Web* čitača (*Web browsers*), kao što su *Netscape Navigator*, *Internet Explorer*, *Opera* ili *Mozilla Firefox*. Jednim klikom miša se prelazi u neki dokument, bez obzira gde se on fizički nalazi.

Razvoj Web-a

Web je nastao u evropskom centru za nuklearna istraživanja (CERN), gde se konsultant Tim Berners-Lee gotovo deceniju bavio problemom stvaranja dobrog hipertekst sistema. Godine1989. u članku *Information Management: A Proposal*, zajedno sa prilogom "HyperText and CERN", predložio je, a 1990. godine i razvio program *WorldWideWeb* kao potpuno grafički orjentisan čitač/editor sa mogućnošću direktnog kreiranja linkova.

Za potrebe sistema prilagodio je jezik SGML (*Standard Generalized Markup Language*), ISO standard za opis izgleda stranice dokumenta i razvio njegovu pojednostavljenu verziju HTML (*HyperText Markup Language*) za opis izgleda hipertekst dokumenata.

Osnovna jedinica sadržaja je Web stranica (*Web page*), koja tehnički predstavlja tekst u jeziku HTML. Da bi se neki dokument ili objekt pronašao koristi se *Hypertext Transfer Protocol* (HTTP), zajedno sa univerzalnim lokatorom resursa (URL).

Prvi Web server je imao Internet adresu **http://info.cern.ch**, funkcionisao je do 2003. godine, nakon čega je zamenjen server, a sam sajt je modernizovan.

Kao prilog razvoju Interneta, 30. aprila 1993. godine CERN je objavio deklaraciju prema kojoj svako može da koristi WWW tehnologiju *besplatno*.

Razvoj Web-a je omogućio razmenu fajlova, informacija, grafike, zvuka, video i drugih objekata nezavisno od hardverske platforme i operativnog sistema.

Jezici na Web-u

Sadržaj Web-a su dokumenti standardizovanog fomata, koji se opisuje posebnim jezicima za opis dokumenata na Web-u (*Markup Languages*). Jezici HTML, XHTML i XML su nastali na osnovu ISO standarda SGML (*Standardized Generalized Markup Language*).

Jezik HTML (*Hypertext Markup Language*) je relativno lak za korišćenje i obezbeđuje dizajnerima Web stranica skup oznaka (*tags*) koje se koriste za formatiranje Web stranica. Opis izgleda stranice je nezavisan od uređaja na kome se Web stranica prikazuje. Na slici 3.14 je primer HTML koda za opis izgleda Web stranice, kao i sam izgled stranice, onako kako ga prikaže Web čitač.

(A) HTML Kod Web stranice

(B) Izgled Web stranice

Slika 3.14 Tekst i izgled primera Web stranice

HTML editori

Iako se za izradu Web stranica može koristiti običan tekst editor, razvijeni su brojni softverski alati, različitih mogućnosti i složenosti. Osnovni programski alati za kreiranje Web stranica često se nazivaju alati za neposrednu izradu Web sadržaja (*Web authoring tools*) ili HTML editori. Ovi alati se koriste za izradu HTML dokumenata i integraciju različitih multimedijskih materijala u jedinstvenu celinu - Web sajt.

Najpoznatiji komercijalni alati su grafički orijentisani editori Adobe *Dreamweaver* i Microsoft *FrontPage*. Postoje brojni besplatni alati (*open source* i *freeware*) različite složenosti, npr. Mozilla *Composer*.

Brojni su i namenski alati za pojednostavljivanje procesa izrade kompletnih Web sajtova, ali i složeni alati, koji elemente sajta čuvaju u bazi podataka, tzv. sistemi za upravljanje sadržajem (*Content Management Systems*, CMS).

Jezik XML

Osim jezika HTML, na Web-u se koristi i jezik XML (*Extensible Markup Language*), koji je razvio konzorcijum W3C sa ciljem da se osim izgleda dokumenata opišu podaci i informacije. Jezik koristi sličnu formu kao HTML, ali nema unapred definisane oznake. Podaci se opisuju u obliku hirerarhije tipova, zajedno sa samim podacima. Naprimer, XML kod dokumenta koji predstavlja poslovnu belešku (*note*) može biti [1]:

```
<?xml version="1.0"?>
<note>
<to>George</to>
<from>Carol</from>
<heading>Just a Reminder</heading>
<body>Don't forget to order the groceries from WebVan!</body>
</note>
```

Drugi primer XML je kod jednog zapisa iz medicinskog kartona [1]:

```
<?xml version="1.0"?>
<list>
<medical record patient id=456 45 3498>
<name>John Q. Williams<name>
<address>52 Oregon Road<address>
<city>Ann Arbor<city>
<state>Michigan<state>
<zip code>45678<zip code>
<doctor name>Frank Lucretis<doctor name>
<list>
```

Softver Web servera omogućava kompjuteru da isporuči klijentskom računaru Web stranice urađene u jeziku HTML tako što pošalje HTTP zahtev.

Osnovne mogućnosti Web servera obuhvataju:

- sigurnosne usluge (autentifikacija)
- protokol za prenos fajlova (*File Transfer Protocol*)
- pretraživanje sajta
- prikupljanje podataka o radu.

Osnovne vrste servera na Web-u su:

- server baze podataka (*database server*), računar koji omogućava pristup informacijama koje su zaapamćene u bazama podataka;
- server za oglase (*ad server*), služi za isporuku ciljnih oglasa – banera;
- server za elektronsku poštu (*e-mail server*), prosleđuje elektronske poruke;
- video server, koji služi za isporuku video spotova.

Najpoznatiji Web serveri su besplatni server otvorenog koda *Apache* i komercijalni Microsoft *Internet Information Server* (IIS).

Web klijent je bilo koji kompjuterski uređaj priključen na Internet koji je sposoban da postavlja HTTP zahteve i da prikazuje HTML stranice. Najčešći Web klijenti su personalni računari, koji koriste operativni sistem *Windows*, *MacIntosh* ili *Linux*.

Web čitač (*browser*) je program čija je osnovna namena prikaz Web stranica. Osim toga, često može da izvršava i druge funkcije, kao npr. upravljanje eletronskom poštom. Najpoznatiji Web čitači su Microsoft *Internet Explorer*, Mozilla *Fairfox*, Google *Chrome* i *Opera*.

3.5. OSNOVNE MOGUĆNOSTI INTERNETA I WEB-A

Internet i Web raspolažu nizom aplikaitivnih rešenja, na kojima se zasnivaju i mnoga rešenja u elektronskoj trgovini:

1. Elektronska pošta (*e-mail*) je Internet aplikacija koja se najviše upotrebljava. Koristi seriju protokola za prenos tekstualnih poruka, obogaćenih slikama, zvukom i video materijalima od jednog Internet korisnika do drugog. Pomoću sistema elektronske pošte mogu se slati fajlovi različitih formata, kao dodaci porukama (*attachments*).

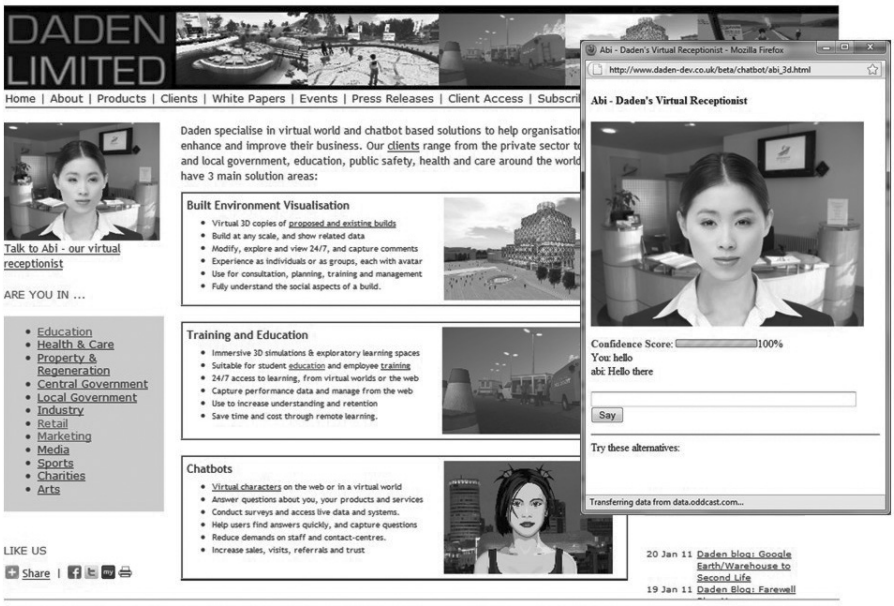
   Vrlo često se javljaju neželjene poruke elektronske pošte (*spam*), koje se često kreiraju i šalju u svrhu marketinga.

2. Razmena poruka (*instant messaging*) omogućava razmenu tekstualnih poruka učesnika gotovo u realnom vremenu, tako da komunikacija liči manje-više na razgovor uživo, koji nije moguć preko sistema elektronske pošte.
3. Pretraživači (*search engines*) identifikuju Web stranice pomoću ključnih reči koje zadaje korisnik, tako da se dobije spisak stranica koje najviše odgovaraju onome što korisnik traži. To je preovlađujući način pronalaženja sadržaja na Web-u, pošto ne postoji uređeni Web katalog.
4. Intelligentni agenti (*web robots* il samo *bots*) su softverski programi koji prikupljaju i/ili filtriraju informacije sa Web-a o nekoj predmetnoj oblasti i zatim daju spisak rezultata rangiranih na više načina.

   Prema nameni, inteligentni Web agenti mogu biti:

   - *search bot* – za pretraživanje (npr. Altavista.com, Webcrowler.com)
   - *shopping bot* – za pomoć u kupovini
   - *Web monitoring bot* – za Web nadzor (monitoring)
   - *news bot* - za izveštavanje
   - *chatterbot* - za govornu ili tekstualnu komunikaciju kroz dijalog (ćaskanje), kao što su poznati programi *Lucy*, *Eve* (eGain.com) i *Alice* (www.alice.com).

   Na slici 3.15 prikazan je vizuelno animirani inteligentni program za ćaskanje (*chatterbot*), koji vodi tekstualnu i glasovnu konverzaciju sa ljudskim sagovornikom, obično u nekoj zamišljenoj ulozi (npr. kao virtuelni recepcioner).



Slika 3.15 Primer inteligentnog agenta za ćaskanje (*chatbot*)

5. Online forumi i programi za ćaskanje (*Chat*) omogućavaju većem boju korisnika da kominiciraju preko kompjutera u realnom vremenu, odnosno simultano razgovaraju.
6. Multimedija u realnom vremen (*Streaming Media*) omogućava da se veći fajlovi, kao što su muzika ili video, pošalju korisnicima tako da ih može koristiti (slušati, gledati) u realnom vremenu, bez prekida, istovremeno dok traje kopiranje na klijentski računar.
7. Kolačići (*Cookies*) su alati koje koriste Web sajtovi u cilju memorisanja podataka o korisniku radi kasnije upotrebe. Predstavljaju male tekstualne fajlove zapamćene u *računaru korisnika*. Sadrži osnovne podatke o korisniku i korisničkom računaru, radi prepoznavanja pri narednim konekcijama.

3.6 PODRŠKA INTERNET-A I WEB-A ELEKTRONSKOJ TRGOVINI

Kao posledica povećanja propusnosti Interneta, pojavile su se nove primene, koje otvaraju nove mogućnosti za elektronsku trgovinu, a odnose se na digitalni sadržaj i Web komunikacije:

1. Web dnevnici (*Blogs*) su lične Web stranice, povezane sa drugim Web stranicama, koje sadrže niz hronološki uređenih priloga autora dnevnika.
2. Distribucija izmena sadržaja Web dokumenata (*Really Simple Syndication*, RSS) je usluga automatskog slanja izmena određenih Web sadržaja putem Interneta.
3. Distribucija multimedijskih sadržaja (*webcasting/podcasting*) je postavljanje audio saržaja na Web, tako da se omogući njihovo reprodukovanje na mobilnim uređajima za reprodukciju, kao što je Apple *iPod*. Velika porast obima upotrebe omogućava njihovo korišćenje u reklamne svrhe.
4. Kolaborativne Web aplikacije (Wikis) omogućavaju kolektivnu izradu i izmene Web stranica radi kreiranja različitih sadržaja, npr. knjiga i encklopedija, kao što je *Wikipedia*.
5. Novi muzički i video servisi

   Pored fotografija, videa i video animacija, pojavile su se nove komercijalne usluge, kao što je video na zahtev (*video on demand*), koji pruža kvalitetniji zvuk i video od radio i televizijskih stanica.
6. Internet telefonija i televizija

   Internet ili *IP telefonija* je opšti izraz za tehnologiju koja koristi Internet, mrežu sa komutacijom paketa i VOIP protokol (*Voice Over Internet Protocol*), za prenos govora preko Interneta i druge vidove audio komunikacije.

7. Videokonferencije na savremenim širokopojasnim vezama i uz pomoć relativno pristupačnih komercijalnih uređaja imaju značajno niže troškove, tako da postaju dostupne većini učesnika, koji na taj način mogu da razmenjuju informacije, uključujući video i audio sadržaje.

   Tele-uranjanje (*tele-immersion*) predstavlja spoj virtualne realnosti i video-konferencije, gde se učesnici vide i mogu da učestvuju u vizuelnim projektima.
8. Online softver i Web servisi, kao što su Web aplikacije, vidžeti (*widgets*) i alatke (*gadgets*).

   Digitalne biblioteke - distribucija aplikativnog softvera, multimedija i drugih usluga na bazi plaćanja preko Application Service Providers (ASP)

   Distribuirana memorija - ASP može da asistira i u prenosu i u memorisanju podataka, raspodeljujući ih različitim, a ne samo jednom serveru.
9. Učenje na daljinu (*Distance Learning*, DL) jedna je od najvećih obrazovnih inicijativa poslednjih godina, nudi *online* kurseve i diplomske programe
10. Mobilne aplikacije e-trgovine (*m-commerce*) omogućavaju kombinovanje govora, podataka, audio i video sadržaja na jednom bežičnom uređaju, kao što je ručni računar ili mobilni telefon, Slika 3.16.

Slika 3.16 Nove generacije mobilnih uređaja u obliku mobilnih telefona (*smartphone*)

Ilustracija: Akamai tehnologije i Web

Poboljšanje Internet performansi se vrši premeštanjem Web sadržaja bliže krajnjim korisnicima, čime se poboljšavaju performanse Web sajta i maksimizuje brzina isporuke sadržaja. Računarstvo ivice (*edge computing*) obezbeđuje balansiranje opterećenja kapaciteta za obradu aplikacija korporativnih i drugih velikih Web servera. Jedna od kompanija koja obezbeđuje ove usluge *Akamai.com*, Slika 3.17. Njene usluge koristi veliki broja kompanija i državnih institucija, kao što su npr. NASDAQ, General Motors, FBI, FedEx, NASA, Yahoo i BestBuy.com.

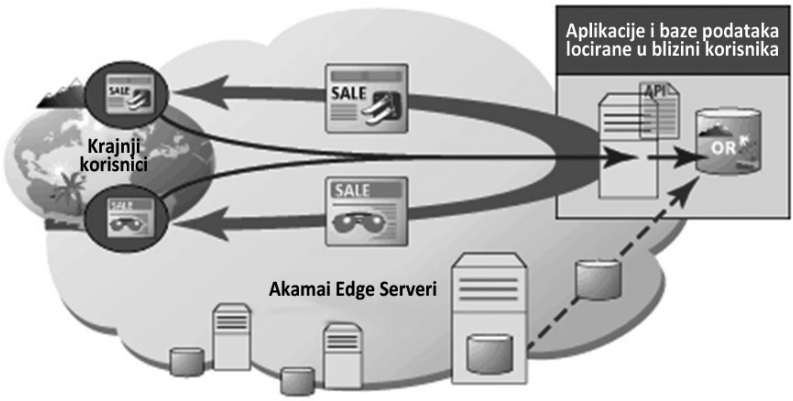
Slika 3.17 Upravljanje rutiranjem

Reč *Akamai* na havajskom znači "pametno" i odnosi se na značajno poboljšanje performansi Interneta programskim upravljanjem ukupnim procesom rutiranja paketa. Pristup poboljšanju Internet performansi sastoji se u [10]:

- eliminisanju dužih puteva, kad god je to moguće, vršenjem replikacije i isporuke sadržaja i aplikacija sa servera koji su blizini krajnjih korisnika širom sveta, umesto sa centralnog servera. Akamai to naziva ovaj isporukom sa "ivice Interneta".
- optimizaciji puteva mapiranjem putanja kroz Internet, kako bi se izbegle problematične tačke, kao i kompresiji sadržaja i replikaciji paketa, kako bi se osigurala brza i kompletna isporuka.

Danas je *Akamai EdgePlatform* jedna od najvećih svetskih platformi distribuiranog računarstva. Predstavlja računarsku mrežu više od 73.000 zaštićenih servera opremljenih sopstvenim softverom i raspoređenih u 70 zemalja, koja se oslanja na primenjenu matematiku i algoritme za rešavanje problema ranjivosti i zagušenja na Internetu.

Serveri su organizovani u približno 1.000 mreža širom sveta, koje nadziru Internet u realnom vremenu i prikupljaju informacije o saobraćaju, zagušenjima, i problematičnim mestima. Akamai koristi ove informacije za optimizaciju puteva i vrši dinamičku replikaciju (umnožavanje kopija) podataka radi brže, pouzdanije i sigurnije isporuke sadržaja i aplikacija, Slika 3.18.



Slika 3.18 Princip računarstva ivice

Osim toga, *Akamai EdgeScape* obezbeđuje oglašavače podacima koje dobija *inteligentnom analizom* baza podataka nastalih praćenjem aktivnosti potrošača na mreži.

3.7 LITERATURA

[1] Laudon K.C., Traver C.G., *E-commerce, business, technology, society*, 3rd Ed, Addison Wesley, 2006

[2] Kurose, J. F., Ross, K. W., *Computer Networking: A Top-Down Approach*, , 2007

[3] http://www.isc.org/solutions/survey

[4] www.merriam-webster.com

[5] http://www.isoc.org/internet/history

[6] www.wikipedia.org

[7] Nelson T., "A File Structure for the Complex, the Changing, and the Indeterminate", *Proceedings of the ACM 20th national conference*, New York, Association for Computing Machinery, 1965.

[8] http://www.internetworldstats.com

[9] www.internet2.edu

[10] www.akamai.com

4. IZGRADNJA WEB SAJTA ELEKTRONSKE TRGOVINE

U ovom poglavlju se objašnjava proces izgradnje Web sajta namenjenog elektronskoj trgovini. Opisuju se faktori koje menadžer treba da razmotri i poslovne odluke, koje je neophodno doneti da bi se Web sajt e-trgovine izgradio, pokrenuo i omogućilo njegovo uspešno poslovanje.

Izgradnja Web sajta e-trgovine za globalno svetsko tržište može biti složen zadatak, zbog čega postoje specijalizovane softverske kompanije, koje se bave izgradnjom i postavljanjem Web sajtova e-trgovine, a često nude i dodatne usluge.

Složenost Web sajta za e-trgovinu proističe iz visokih performansi koje treba postići za zadovoljenje velikog broja klijentskih zahteva u višekorisničkom okruženju. Osnovna mera performansi je *vreme odziva* sajta na zahtev korisnika [1].

4.1. SISTEMSKI PRISTUP IZGRADNJI WEB SAJTA E-TRGOVINE

Razvoj Web sajta e-trgovine predstavlja izgradnju specifičnog softverskog proizvoda, transakcionog informacionog sistema u Web tehnologiji. Za izgradnju uspešnog sajta potrebna su znanja o poslovanju, informacionim tehnologijama i društvenim odnosima, tako da u projektu razvoja ne učestvuju samo informatičari, već je potreban timski rad i saradnja više različitih struktura kompanije.

Najvažniji zahtevi u upravljanju izgradnjom uspešnog sajta e-trgovine su (1) potpuno razumevanje poslovnih ciljeva i (2) stručno znanje za pravilan izbor tehnologije za postizanje tih ciljeva.

Poslovni ciljevi se definišu izradom plana razvoja sajta e-trgovine konkretne kompanije. Stručna znanja podrazumevaju poznavanje i razumevanje potrebnih elemenata infrastrukture e-trgovine.

Planiranje razvoja Web sajta i razumevanje osnovnih infrastrukturnih pitanja e-trgovine su neophodni, bez obzira da li se razvoj vrši sopstvenim snagama ili se razvoj i rad sajta poveravaju specijalizovanoj kompaniji.

4.1.1 Komponente procesa izgradnje Web sajta

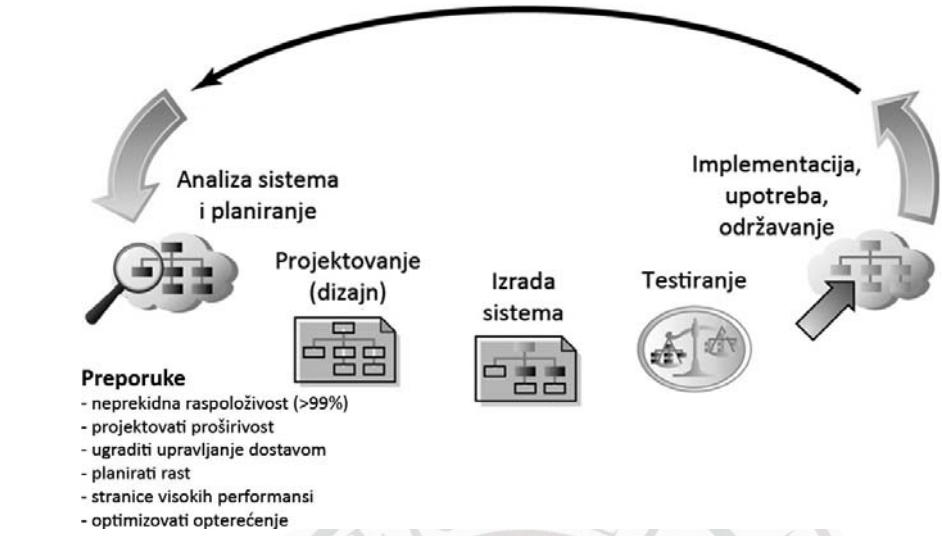
Menadžment kompanije definiše poslovne ciljeve, postavlja funkcionalne zahteve i odobrava resurse za razvoj sajta e-trgovine, pre svega finansijska sredstva i rokove. Pokretanje projekta razvoja postavlja pred odgovornog menadžera zadatak formiranja razvojnog tima, koji će omogućiti donošenje kompetentnih odluka o svim ostalim faktorima razvoja, prikazanim na Sl. 4.1 [1].

Slika 4.1 Elementi izgradnje Web sajta

Sam izbor tehnologije (hardver, softver i telekomunikacije) vrši se na osnovu predvidivih potreba i zahteva budućih klijenata, kojima treba omogućiti da što lakše pronađu, pregledaju, kupe i brzo dobiju traženi proizvod ili uslugu, čemu će doprineti i odgovarajući dizajn Web sajta.

4.1.2 Planiranje i životni ciklus razvoja sistema (SDLC)

Nakon definisanja problema, sledeći korak je izrada planskog dokumenta. Sistemski pristup razvoju složenih sistema podrazumeva izbor proverene metodologije razvoja, koja obuhvata sve faze životnog ciklusa sistema prikazanih na Sl. 4.1 [1].



Slika 4.2 Životni ciklus razvoja sistema (Web sajta e-trgovine)

Životni ciklus sistema predstavlja niz stanja ili faza kroz koje sistemi prolaze. Osnovne faze svakog sistema su nastajanje, *razvoj*, zrelost i opadanje. Pojam životnog ciklusa razvoja sistema (*System Development Life Cycle*, SDLC) odnosi se na razvojnu fazu kompletnog životnog ciklusa sistema i često poistovećuje sa metodologijom razvoja [2],[3].

Životni ciklus razvoja sistema ili softvera je pojam koji se, u sistemskom inženjerstvu, informacionim sistemima i softverskom inženjerstvu, odnosi na proces stvaranja ili izmena sistema, kao i modele i metodologije koji se koriste u njihovom razvoju [1].

U softverskom inženjerstvu se razmatra veći broj metodologija ili modela razvoja softvera, kao što su model vodopada, koji predstavlja izvorni SDLC metod, model brzog razvoja aplikacija (*Rapid Application Development*, RAD), model zajedničkog razvoja aplikacija (*Joint Application Development*, JAD), model vodoskoka, spiralni model, itd. [2], [3]. U praksi se pokazalo da je razvoj svakog sistema specifičan problem i da se najbolji rezultati postižu kombinovanjem više modela razvoja, dnosno primenom hibridne metodologije.

U oblasti upravljanja projektima, životni ciklus razvoja opisuje faze projekta razvoja informacionog sistema, od početne studije izvodljivosti do eksploatacije i održavanja razvijene aplikacije.

Svi modeli razvoja predviđaju izradu različite dokumentacije, kao važan deo procesa razvoja sitema. Usvajanje poznate metodologije pomaže u izradi standardnih dokumenata, kojim se na razumljiv način izveštava viši menadžment o stepenu dostizanja ciljeva, važnim kontrolnim tačkama projekta razvoja i upotrebi resursa.

Iako su neki metodi pogodniji za projekte određene vrste, pokazalo se da je poštovanje plana razvoja najvažnije za uspeh projekta.

Osnovne faze životnog ciklusa razvoja informacionog sistema su [2], [3]:

1. analiza sistema i planiranje
2. projektovanje (dizajn) sistema
3. izrada sistema
4. testiranje sistema
5. implementacija

Specifičnosti razvoja složenijih Web sajtova, u koje spadaju sajtovi e-trgovine, ističu pojedine aktivnosti planiranja i implementacije, tako da se razvoj Web sajta posmatra kroz sledeće glavne faze [4], [5]:

1. Definisanje i planiranje sajta
2. Izrada informacione arhitekture
3. Projektovanje sajta (*design*)
4. Izrada sajta (*construction*)
5. Promocija sajta (*marketing*)
6. Praćenje, ocenjivanje i održavanje

4.1.3 Sistemska analiza - poslovni ciljevi, funkcije i informacioni zahtevi

Analiza sistema i planiranje treba da odgovori na pitanje o tome šta sajt e-trgovine treba da radi. Prethodno treba identifikovati poslovne strategije i izabrati poslovni model, koji će omogućiti postizanje osnovnih ciljeva.

Jedan od načina da se započne proces razvoja je identifikacija specifičnih poslovnih ciljeva Web sajta, a zatim izrada spiska funkcija sistema i odgovarajućih informacionih zahteva.

Poslovni ciljevi predstavljaju spisak funkcija koje Web sajt e-trgovine treba da realizuje. Funkcije sistema su spisak mogućnosti informacionog sistema potrebnih za postizanje njegovih poslovnih ciljeva. Informacioni zahtevi sistema su informacioni elementi koje sistem mora da proizvede za postizanje poslovnih ciljeva.

Zadatak menadžera je da obezbedi spisak ciljeva i poslovnih funkcija namenjen projektantima i programerima, kako bi znali šta se od njih očekuje da urade.

Tabela 4.1 opisuje neke osnovne poslovne ciljeve, funkcije sistema i informacione zahteve tipičnog sajta e-prodaje. Kao što se iz tabele vidi, sajt e-prodaje treba da obezbedi postizanje devet osnovnih poslovnih ciljeva [1]. Ove ciljeve treba prevesti u opis funkcija sistema, odnosno u skup preciznih informacionih zahteva.

Tabela 4.1 Sistemska analiza tipičnog sajta e-trgovine: poslovni ciljevi, sistemske funkcije i informacioni zahtevi

Poslovni cilj	Sistemska funkcija	Informacioni zahtevi
Prikaz proizvoda	Digitalni katalog	Dinamički tekst i grafički katalog
Obezbeđenje informacija o proizvodu (sadržaj)	Baza podataka o proizvodima	Opisi proizvoda, skladišni brojevi, nivoi zaliha
Personalizacija / kastomizacija proizvoda	Praćenje korisnika na licu mesta	Dnevnik sajta za svaku posetu kupca; *data mining* metodi za identifikaciju zajedničkih puteva klijenata i odgovarajućih odgovora
Izvršenje transakcija	Korpa za kupovinu i sistem plaćanja	Sigurna naplata kreditnih kartica; više opcija plaćanja
Akumulacija informacija o klijentima	Baza podataka korisnika	Naziv, adresa, telefon i e-mail za sve kupce; *online* registracija korisnika
Obezbeđenje korisničke podrške nakon prodaje	Baza podataka o prodaji	ID klijenta, proizvoda, datum uplate, datum isporuke
Koordinacija programa marketinga i oglašavanja	Serveri za reklame (*Ad server*) i e-poštu; programi za upravljanje marketinškim kampanjama	Dnevnik ponašanja sajta za posetioce i kupce vezane za kampanje putem e-pošte i reklamnih banera
Razumevanje efektivnosti marketinga	Sistem za praćenje i analizu rada sajta (*site tracking and reporting*)	Broj jedinstvenih posetilaca, posećenih strana, kupljenih proizvoda, identifikovanih u marketing kampanji
Obezbeđenje proizvodnje i veze sa dobavljačima	Sistem za upravljanje zalihama (*inventory manaqement*)	Nivoa proizvoda i zaliha, ID dobavljača i kontakt, podaci o narudžbama po proizvodu

Konkretni informacioni zahtevi se obično definišu znatno detaljnije nego u Tabeli 4.1. Poslovni ciljevi sajta e-prodaje su slični ciljevima običnih prodavnica, ali postoje i razlike u funkcijama sistema i informacionim zahtevima: kod sajta e-prodaje, poslovni ciljevi moraju biti u potpunosti realizovani u digitalnom obliku, bez korišćenja prodajnih objekata ili prodavaca, dvadeset četiri sata dnevno, sedam dana u nedelji.

Analiza je proces usmeren na ispitivanje problema i zahteva, koji se rešavaju u sledećoj fazi razvoja posmatranog sistema, sajta namenjenog e-trgovini.

4.1.4 Projektovanje sistema (*design*) - hardver i softver

Nakon što su identifikovani poslovni ciljevi i sistemske funkcije i sastavljena lista preciznih informacionih zahteva (npr. prema tabeli 4.1), može se razmotriti način realizacije

ovih funkcija. Rezultat faze projektovanja je specifikacija sistema - opis glavnih komponenti u sistemu i njihovih međusobnih odnosa.

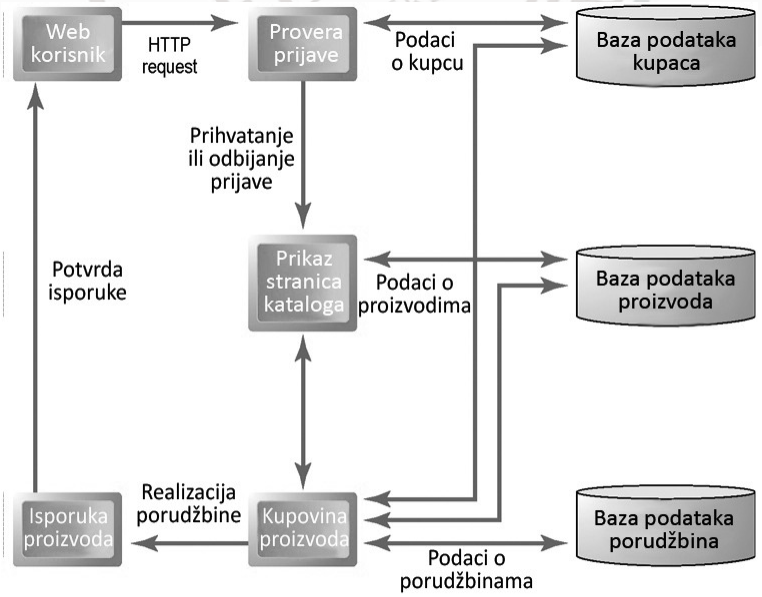
Termin projektovanje (*design*) se odnosi na proces kreiranje nečega što ima namenu, npr. informacionog sistema ili Web sajta e-trgovine. Projektovanje Web sajta e-trgovine je proces kreiranja konceptualnog rešenja koje zadovoljava postavljene zahteve, ali ne i načina njegove implementacije.

Projektovanje sistema se može podeliti na dve komponente: logički i fizički dizajn. Logički dizajn uključuje dijagram toka podataka, koji opisuje protok informacija na sajtu e-trgovine, funkcije obrade koje se moraju biti izvršiti, kao i bazu podataka koja će se koristiti. Logički dizajn takođe uključuje opis zaštite podataka i procedure oporavka koje se pokreću u slučaju otkaza, kao i kontrole koje će se sprovoditi.

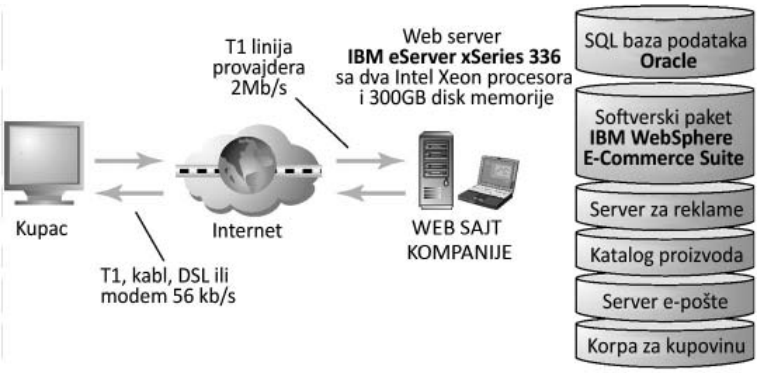
Fizički dizajn prevodi logički dizajn u fizičke komponente. Na primer, fizički dizajn detalja konkretnog modela servera koji se kupuje, softver koji će se koristiti, brzinu telekomunikacionog linka koji će biti potreban, način izrade rezervnih kopija i zaštite od stranih lica, itd.

Na slici 4.3(a) prikazan je dijagram toka podataka visokog nivoa za jednostavan logički dizajn rudimentarnog Web sajta, koji isporučuje HTML stranice kataloga kao odgovor na HTTP zahteve klijentskog čitača.

Slika 4.3(b) prikazuje odgovarajući fizički dizajn istog Web sajta. Svaki od glavnih procesa se može podeliti na nižem nivou projektovanja, koji je mnogo precizniji u identifikaciji tačnog toka informacija i upotrebljene opreme.



(a) Logički dizajn - dijagram toka podataka jednostavnog Web sajta e-trgovine



(b) Fizički dizajn - hardver i softver za realizaciju jednostavnog Web sajta e-trgovine

Slika 4.3 Logički i fizički dizajn jednostavnog Web sajta

4.1.5 Realizacija sistema - sopstveni razvoj ili izmeštanje razvoja

U fazi projektovanja realizovan je i dokumentovan logički i fizički dizajn (projekt) Web sajta e-trgovine. U fazi realizacije ili izrade sistema (*building*), razmatraju se moguće varijante organizacije razvoja i funkcionisanja sajta, slika 4.4.

Razvoj sajta se može u celini prepustiti nekoj firmi (*outsourcing*, koji uključuje i analizu i projektovanje sistema) ili realizovati u okviru kompanije (*in-house*, sopstvenim snagama). Izmeštanje razvoja znači angažovanje spoljne firme za usluge razvoja i izrade sajta, koje ne mogu da realizuju sopstveni kadrovi.

Funkcionisanje sajta e-trgovine može se odvijati na sopstvenim serverima ili na serverima firme specijalizovane za pružanje *Web hosting* usluga.

Postoje firme koje mogu da ponude sve usluge razvoja i funkcionisanja Web sajta, dok su neke specijalizovane samo za proizvodnju softvera ili *Web hosting*.

Sopstveni razvoj zahteva stručni informatički kadar različitih specijalnosti (projektanti, programeri, Web dizajneri i menadžeri), računarsku opremu i softverske alate. Softverski alati mogu biti od osnovnih (*Adobe Dreamweaver*, *Microsoft Visual Studio*) do posebno pripremljenih kompleksnih alata za izgradnju složenih sajtova visokih performansi.

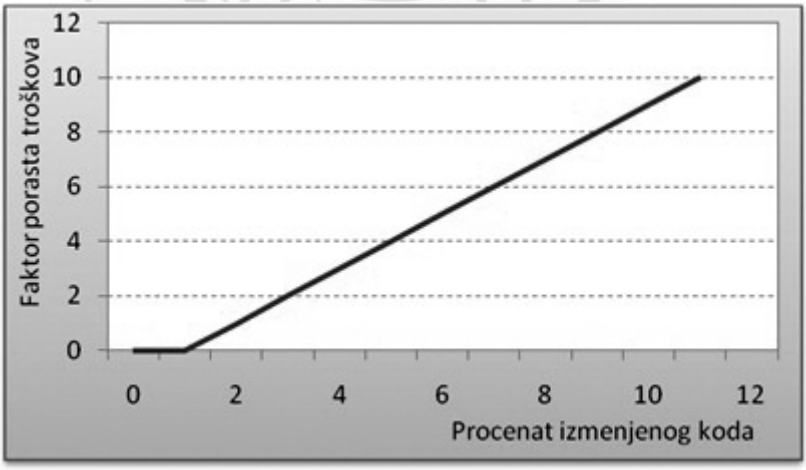
Nedostatak sopstvenog razvoja su rizici vezani za realizaciju složenih funkcija sajta, kao što su korpa za kupovinu, obrada kreditnih kartica, upravljanje zalihama i obrada računa. Sopstvena rešenja mogu da ponavljaju korake razvoja koje su drugi već završili, dok istovremeno učenje i razvoj odlažu početak poslovanja.

Slika 4.4 Varijante organizacije izgradnje i funkcionisanja Web sajta

Prednosti sopstvenog razvoja su izrada sajta u skladu sa sopstvenim potrebama i usvajanje novih tehnologija, što kasnije omogućava brže prilagođavanje sajta promenama poslovnog okruženja.

Prednost nabavke skupog namenskog paketa za izgradnju sajta je korišćenje najsavremenijeg i dobro ispitanog softvera. U tom slučaju se na tržište može izaći ranije, iako ne treba zanemariti da je i za izbor potrebno određeno vreme, koje se koristi za analizu i ocenu većeg broja različitih softverskih paketa.

Prilagođavanje programskih paketa (*customization*), kao i sve druge softverske izmene, takođe se može vršiti sopstvenim snagama ili angažovanjem spoljnih saradnika. Svaka izmena *eksponencijalno* povećava ukupne troškove, slika 4.5 [1].



Slika 4.5 – Troškovi prilagođavanja softverskih paketa e-trgovine

Prodavci koji imaju soptvene maloprodajne objekte obično samostalno projektuju sajtove e-prodavnica, jer već imaju inforrmatički kadar i dosta kapitala uloženog u informacione tehnologije. Spoljne saradnike koriste uglavnom kao isporučioce opreme i konsultante u razvoju složenijih sajtova e-trgovine.

Male kompanije, koje tek traže svoje mesto na tržištu, počinju od početka sopstvenim snagama radi smanjenja troškova. Srednje kompanije obično nabavljaju i modifikuju neko postojeće komercijalno rešenje, dok najmanje kompanije koriste gotove šablone (*template*s) za izgradnju jednostavnih e-prodavnica.

Postavljanje sajta najčešće se vrši na serveru nekog Internet provajdera, korišćenjem standardne usluge *Web hosting*-a. Provajder preuzima odgovornost za neprekidno funkcionisanje i dostupnost sajta 24 časa dnevno. Još jedna usluga koju nude Internet provajderi je *co-location*, mogućnost fizičkog postavljanja sopstvenog servera u obezbeđenu serversku salu provajdera, pri čemu vlasnik servera zadržava potpunu kontrolu nad njegovim funkcionisanjem.

Nedostatak korišćenja spoljne usluge je mogućnost da potrebe prerastu tehničke mogućnosti *hosting* kompanije, što je ponekad razlog izgradnje sopstvene serverske infrastrukture, odnosno objekata i komunikacionih linija, kao i zapošljavanje informatičkig kadra i izgradnju sistema bezbednosti i zaštite podataka.

4.1.6 Testiranje sistema

Testiranje komponenti sistema vrši se već u toku njihovog razvoja, ali je po završetku sistema potrebno sistematski testirati funkcionisanje svake komponente sistema (*unit testing*) i sistema u celini *(system testing*). Testiranje celokupnog sistema podrazumeva testiranje svih mogućih načina upotrebe, odnosno puteva kroz sistem koje korisnik može da realizuje.

Konačni test prihvatljivosti sajta e-trgovine (*acceptance testing*) vrše ključni menadžeri firme (zaduženi za marketing, proizvodnju, prodaju) tako što normalno koriste sistem instaliran na serveru za testiranje. Test prihvatljivosti služi za potvrdu ostvarenja postavljenih poslovnih ciljeva kroz rad sistema.

Ponekad se potcenjuju troškovi testiranja i ponovne izgradnje sistema, koji mogu da angažuju i više od polovine ukupnih napora u razvoju softvera.

4.1.7 Implementacija i održavanje

Većina ljudi pogrešno smatra da se proces završava nakon instalacije informacionog sistema. U stvari, nakon završetka procesa razvoja, radni vek sistema tek počinje. Informacioni sistem u toku rada može da otkaže iz različitih razloga, većinom nepredvidivih.

Informacioni sistemi se moraju stalno proveravati, testirati i popravljati. Održavanje sistema je od vitalnog značaja, ali se na njegove troškove ponekad ne računa. Načelno, godišnji troškovi održavanja sistema su približno jednaki troškovima razvoja, osim za veoma velike sajtove, kod kojih ekonomija obima može smanjiti udeo održavanja.

Osnovni uzrok visoke cene održavanja sajta e-trgovine je njegova dinamičnost, za razliku od sistema za obračun plata i sličnih relativno statičnih aplikacija.

Neke studije tradicionalnih sistema održavanja ustanovile su da se 20% vremena posvećuje otklanjanju grešaka u kodu i reagovanju na vanredne situacije, npr. otkaz zbog instalacije nove opreme. Za promene i izveštajima, fajlovima podataka, kao i linkovima ka serverskim bazama podataka utroši se još 20% vremena. Preostalih 60% vremena održavanja utroši se na opštu administraciju (promene proizvoda i cena u katalogu) i vršenje izmena i poboljšanja sistema [1].

Sajtovi e-trgovine nikada nisu završeni: uvek su u procesu izgradnje i obnavljanja. Oni su mnogo dinamičniji nego sistemi za obračun plata. Dugoročni uspeh sajt e-trgovine će zavisiti od posebnog tima zaposlenih (tzv. *Web tim*), čiji je jedini posao je da prati i prilagodi sajt promenljivim tržišnim uslovima. Web tim mora biti višestruko kvalifikovan, teko da obično uključuje programere, dizajnere i menadžere povučene iz marketinga, proizvodnje, prodaje i podrške.

Jedan od osnovnih zadataka Web tima je analiza povratnih informacija od kupaca i odgovaranje na njihova pitanja.

Važan zadatak je izrada plana sistematskog praćenja i testiranja sajta, radi obezbeđenja ispravnosti svih linkova, tačnosti cena i ažurirnosti stranica. Sistematičnost je neophodna, posebno za Web sajtove velikih e-prodavnica, koje mogu da imaju hiljade međusobno povezanih Web stranica.

Ostali važni zadaci Web tima su *benchmarking*, proces u kome se sajt upoređuje sa konkurentskim po brzini odziva, kvalitetu rasporeda i dizajna, ažurnosti podataka o proizvodima i cenama, kao i promocija sajta.

4.1.8 Faktori koji utiču na optimizaciju performansi Web sajta

Svrha Web sajta je prikaz sadržaja i obezbeđenje kupcima bržeg i pouzdanijeg vršenja transakcija. Što se pouzdanije i brže ova dva cilja realizuju, Web sajt e- trgovine je efikasniji.

Optimizacija performansi Web sajta je složena i obuhvata najmanje tri grupe faktora: *sadržaj* stranica, proces *generisanja* stranica i proces *isporuke* stranica, slika 4.6.

Slika 4.6 – Faktori optimizacije Web sajta

U ovom poglavlju se razmatra izbor softvera i hardvera u procesu izgradnje sajta e-trgovine, što predstavlja važan faktor u optimizaciji Web sajtova.

Upotreba efikasnih HTML stilova i tehnika dizajna i sadržaja stranica može znatno da smanji vreme odziva, kao i korišćenje efikasnije grafike i izbegavanje nepotrebnih veza ka drugim stranicama u okviru sajta.

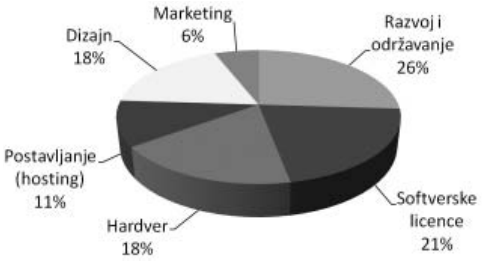
Brzina generisanja Web stranica može se poboljšati uvođenjem zasebnih servera za izvršavanje namenskih funkcija (kao što su generisanje statičkih stranica, aplikativna logika, serveri medija, serveri baza podataka), kao i korišćenjem različitih alata za ubrzanje tih servera.

Isporuka sadržaja može se ubrzati korišćenjem usluga keširanja prometa, neke globalne mreže za isporuku sadržaja kao što je *Akamai* ili specijalizovane mreže poput kompanije *RealNetworks*, kao i povećanjem lokalnog protoka.

4.1.9 Troškovi razvoja Web sajta

Iznos finsijskih sredstva za razvoj Web sajta zavisi od od odobrenog budžeta, kao i od očekivanog tržišta. Na slici 4.7 prikazana je tipična struktura troškova razvoja Web sajta, prema istraživanju izvršenom na uzorku od 125 menadžera Web sajtova [1].

Troškovi tehnologije iznose oko 75% ukupnih troškova (razvoj, rad i održavanje). Za projektovanje i razvoj sadržaja izdvaja se oko 18%, a za marketing sajta oko 6% ukupno raspoloživih sredstava.



Slika 4.7 – Tipična struktura ulaganja u Web sajt e-trgovine

4.2. IZBOR SERVERSKOG SOFTVERA

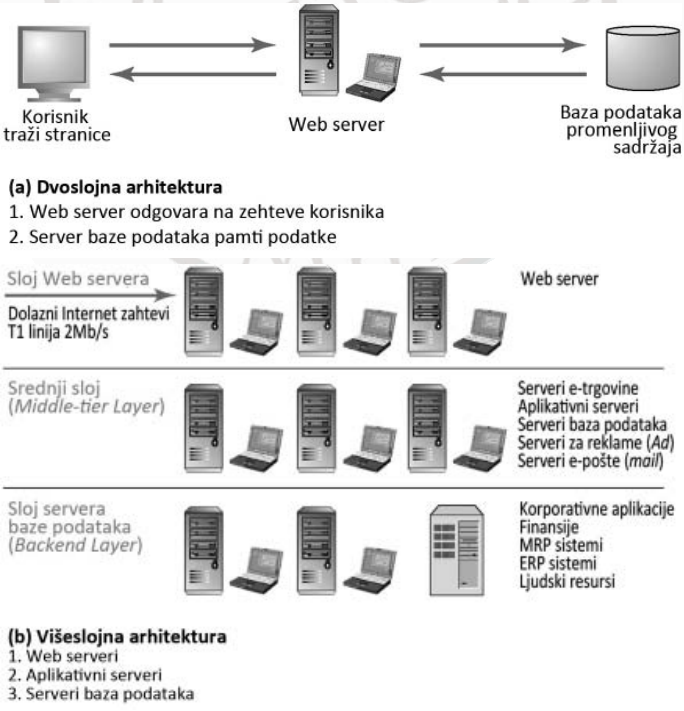
Funkcionisanje sajta e-trgovine pre svega zavisi od sistemskog i aplikativnog softvera. Jedan od važnih zadataka menadžera projekta je izbor serverskog softvera, koji zavisi od izabrane arhitekture Web sajta e-trgovine.

4.2.1 Jednostavna ili višeslojna arhitektura Web sajta

Arhitektura Web sajta je konfiguracija softvera, hardvera i zadataka informacionog sistema neophodna za postizanja zadane funkcionalnosti.

Sistemska arhitektura može biti dvoslojna ili višeslojna, kao na slici 4.8. Dvoslojna (*two-tier*) arhitektura je kada se sistem sastoji samo od Web servera, koji odgovara na zahteve klijenta za Web stranicama i servera baze podataka, koji obezbeđuje memorisanje podataka, slika 4.8(a).

U višeslojnoj (*multi-tier*) arhitekturi, slika 4.8 (b), Web server je povezan sa srednjim slojem (*middleware*), koji obuhvata niz aplikativih servera za izvršavanje posebnih zadataka, kao i sa zadnjim slojem (*backend*), koga čine postojeći korporativni informacioni sistemi sa nasleđenim bazama podataka (*legacy databases*).



Slika 4.8 – Osnovne arhitekture Web sajta e-trgovine

4.2.2 Softver Web servera

Softver Web servera odgovara na zahteve klijenata za HTML i XML stranicama. Osnovne funkcije Web servera su:

- Obrada HTTP zahteva - prijem i odgovor na zahteve klijenata za HTML stranicama;
- Bezbednosni servisi (*Secure Sockets Layer*) - verifikacija imena i lozinke korisnika, obrada sertifikata i javnih i privatnih ključeva neophodnih za obradu kreditnih kartica i druge bezbednosne funkcije;
- Prenos fajlova (*File Transfer Protocol*) - prenos veoma velikih fajlova putem Interneta;
- Pretraživanje (*search engine*) - indeksiranje sadržaja Web sajta i pretraživanje po ključnim rečima;
- Prikupljanje podataka (*data capture*) - dnevnik svih operacija, posebno poseta klijenata (vreme, trajanje i način dolaska);
- Elektronska pošta (*e-mail*) - može da prima, šalje i čuva poruke elektronske pošte;
- Alati za upravljanje sajtom (*site management tools*) - računanje i prikaz statističkih podataka, kao što je broj jednistvenih posetilaca, broj zahteva za stranicama, poreklo zahteva, kao i provera ispravnosti postojećih linkova na stranicama i identifikacija nevažećih fajlova.

Izbor Web servera povezan je sa izborom operativnog sistema serverskog računara. Najčešći operativni sistemi su različite verzije komercijalnog sistema *Microsoft Windows* i (besplatnog) softvera otvorenog koda *Linux*.

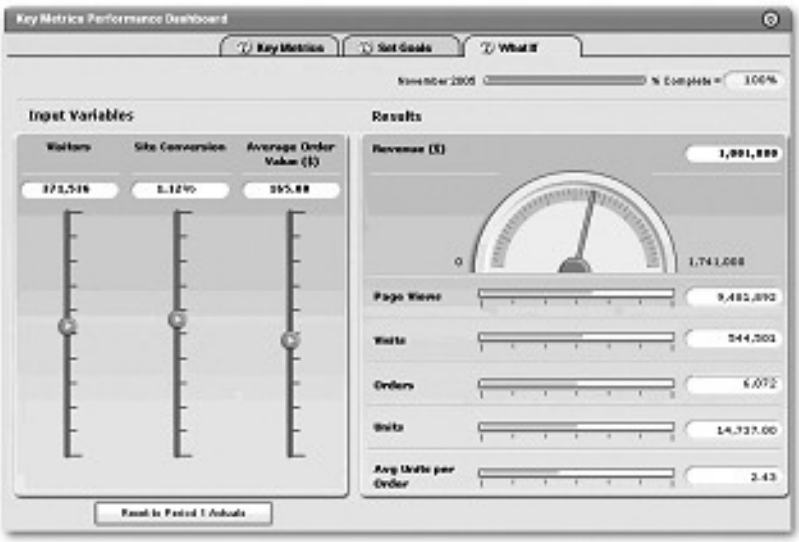
Najzastupljeniji Web server je *Apache*, softver otvorenog koda, koji zauzima gotovo polovinu svetskog tržišta i čije verzije postoje za sve važnije operativne sisteme, uključujući i komercijalni *Microsoft Windows*.

Svi operativni sistemi iz porodice *Microsoft Windows* koji imaju serverske funkcije, već imaju ugrađen sopstveni Web server, koji se naziva *Internet Information Server*.

4.2.3 Alati za upravljanje Web sajtom

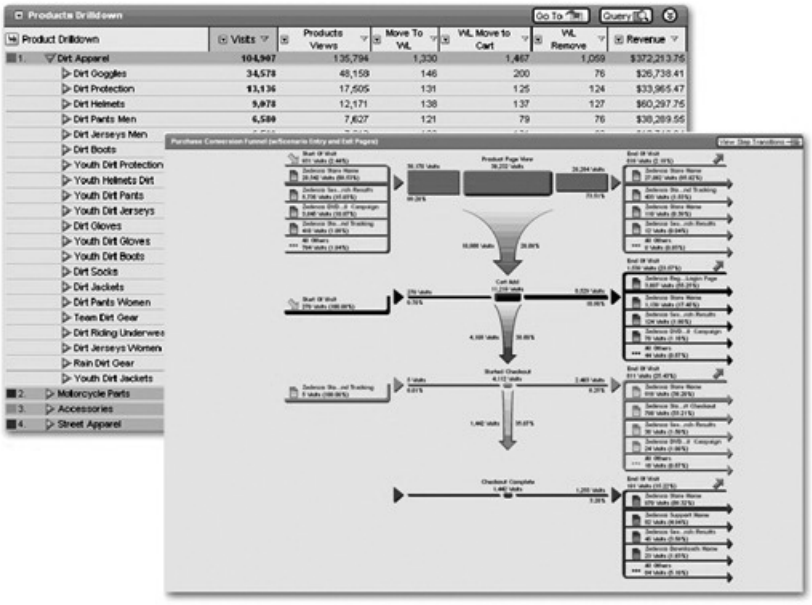
Osnovne alate za upravljanje Web sajtom, koji obuhvataju proveru ispravnosti linkova i otkrivanje nevažećih fajlova, omogućavaju svi Web serveri.

Složeniji alati za upravljanje, kao što su *Web Trends Analytics* [1], [6] i *Google Analytics* [7] omogućavaju nadzor i vizualizaciju podataka o kupovini, praćenje efekata marketinških kampanja i slično. Na slici 4.9 prikazan je *Web Trrends* interfejs za praćenje osnovnih pokazatelja (metrike) Web sajta e-trgovine.



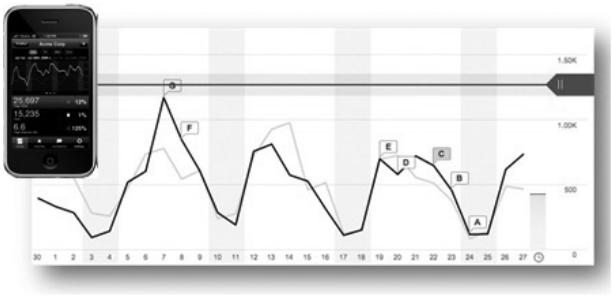
Slika 4.9 WebTrends upravljačka tabla za osnovne pokazatelje rada Web sajta

Moguće je konfigurisati sopstvene izveštaje, npr. kao što su izveštaji o ponašanju kupaca prilikom kupovine određenih proizvoda, odnosno koristiti ponuđene analitičke izveštaje sa veoma preglednom vizualizacijom, Slika 4.10.



Slika 4.10 WebTrends analitički izveštaji

Na slici 4.11 je prikaz mogućnosti izveštavanja u realnom vremenu, odnosno upozorenja preko mobilnog uređaja kada pokazatelji rada Web sajta e-trgovine, kao što je npr. broj online posetilaca Web sajta, dostignu zadane ciljne vrednosti.



Slika 4.11 WebTrends softver interfejs za mobilne uređaje

4.2.4 Alati za dinamičko generisanje Web stranica

Dinamičko generisanje Web stranica se vrši kada sadržaj Web stranice nije eksplicitno kodiran u HTML kodu, već se generiše programskim putem ili memoriše kao objekat u bazi podataka. Kad je potrebno, Web server izračunava ili uzima sadržaj stranice iz baze podataka sajta i konstruiše HTML kod tražene stranice.

Razdvajanje konkretnog sadržaja stranice (tekst, slika, video) od Web dizajna omogućava lakše izmene neprofesionalcima, koji ne znaju HTML. Na taj način se za stalne izmene sadržaja sajta mogu angažovati oni zaposleni koji su inače odgovorni za određeni sadržaj.

Alati za dinamičko generisanje stranica obuhvataju različite Web tehnologije, kao što su CGI (*Common Gateway Interface*), ASP (*Active Server Pages*), JSP (*Java Server Pages*), itd.

Dinamičko generisanje stranica snižava cenu ažuriranja podataka (npr. cena), omogućava laku *online* segmentaciju tržišta i besplatnu diskriminaciju cena.

4.2.5 Aplikativni serveri

Aplikativni Web serveri su softverski alati koji realizuju specifične poslovne funkcije potrebne Web sajtu e-trgovine, pre svega:

- prikaz kataloga proizvoda
- obradu transakcija
- server audio i video materijala
- aukcijski server
- B2B server

Aplikativni serveri predstavljaju softver srednjeg sloja (*middleware*), Slika 4.8. Postoji više *vrsta* aplikativnih servera, sa različitim funkcijama, Tabela 4.2.

Tabela 4.2 – Vrste aplikativnih servera i njihove funkcije

Aplikativni server	Funkcija
Prikaz kataloga	Obezbeđenje baze podataka s opisima i cenama proizvoda
Obrada transakcija – korpa za kupovinu (*shopping cart*)	Prijem narudžbi i realizacija plaćanja
Server lista	Kreiranje i održavanje mailing lista i upravljanje marketinškim kampanjama
Proxy server	Nadgledanje i kontrola pristupa Web serveru i zaštitni zid
Mail server	Upravljanje elektronskom poštom na Internetu
Audio/video server	Pamćenje i isporuka emitovanih sadržaja (*streaming media*)
Chat server	Okruženje za tekstualnu i audio komunikaciju s kupcima u realnom vremenu
News server	Povezivanje i prikaz Internet vesti
Fax server	Prijem i slanje telefaks poruka poomoću Web servera
Groupware server	Stvara okruženje za saradnju radnih grupa
Database server	Skladištenje informacija o kupcima, proizvodima i cenama
Ad server	Održavanje baze podataka reklamnih banera, koja omogućava prilagođen i personalizovan prikaz reklama na osnovu ponašanja i osobina potrošača
Aukcijski server	Obezbeđenje okruženja za vršenje transakcija na online aukcijama
B2B Server	Realizacija kupovine, prodaje i povezivanje tržišta za komercijalne transakcije

Postoji veliki broj komercijalnih i besplatnih aplikativnih Web servera, koji se koriste u funkcijama prodaje, za povezivanje sa partnerima i njhihovim lancima snabdevanja i pronalaženje dobavljača za određene delove ili sklopove.

4.2.6 Funkcije servera elektronske trgovine

Server e-trgovine (*e-Commerce Merchant Server*) je softver koji omogućava osnovnu funkcionalnost potrebnu za *online* prodaju. Osnovne funkcije uključuju:

- Prikaz *online* kataloga proizvoda koji se nude na Web sajtu;

- Preuzimanje narudžbine *online*, tako da kupci mogu da odvajaju na stranu proizvode koje žele da kupe, pregledaju šta su naručili i da realizuju svoju narudžbinu aktiviranjem tastera na Web stranici;
- *Online* obradu kreditnih kartica, koja obezbeđuje verifikaciju kartice i bezbedan prenos navedene sume novca na račun e-prodavca.

Katalog proizvoda (online catalog)

Ponuda proizvoda i usluga na Web sajtu se obično daje u obliku liste ili online kataloga proizvoda, koji sadrži osnovne informacije o proizvodima i njihovu cenu. Zavisno od vrste i broja proizvoda, kao i veličine kompanije, katalog može da sadrži i fotografije, animacije, zvučne ilustracije i video snimke demonstracije proizvoda, kao i mogućnost uspostavljanja direktne tekstualne ili videokonferencijske komunikacije sa predstavnicima kompanije.

Katalog proizvoda se obično relizuje preko Web stranica povezanih sa bazama podataka u kojima se čuvaju svi neophodni podaci kataloga, uključujući slike i druge multimedijske sadržaje.

Korpa za kupovinu (shopping cart)

Korpa za kupovinu je popularan naziv za programski interfejs namenjen izboru proizvoda i udobnom formiranju narudžbe, koji je realizovan tako da kupovina proizvoda što više podseća na kupovinu u realnoj prodavnici.

Kupovina se može realizovati jednostavnim pritiskom na taster, kojim se pokreće funkcija plaćanja preko Interneta, najčešće pomoću softvera za obradu kreditnih kartica. Softver korpe za kupovinu je deo serverskog softvera i nalazi se na Web serveru.

Obrada kreditnih kartica

Softver za obradu kreditnih kartica realizuje funkciju plaćanja tako što vrši proveru kreditne kartice kupca, nakon čega zadužuje karticu za iznos vrednosti narudžbe, koji prenosi na račun prodavca.

Softverski paketi e-trgovine najčešće obezbeđuju ovu funkciju, koja se realizuje u saradnji sa bankama i posrednicima koji podržavaju korišćenje kreditnih kartica.

4.2.7 Softverski paketi elektronske trgovine

Softverski paketi elektronske trgovine (e-*Commerce Suites*) nude integrisano okruženje, koje pruža većinu ili sve funkcije i neophodne resurse potrebne za razvoj složenih Web sajtova orjentisanih ka kupcima.

U odnosu na cene i performanse, postoje tri klase paketa - osnovna, srednja i visoka klasa komercijalnih softverskih paketa.

Na tržištu postoji veliki izbor besplatnih i komercijalnih paketa e-trgovine osnovne (niže) klase, kao što su [9]:

- *Yahoo's Small Business Merchant Solutions*, koji omogućava kreiranje sajta, hosting, plaćanje i analitičke funkcije, slika 4.12.
- *Freemerchant* je serverski softver korpe za kupovinu, sa obaveznom uslugom hostinga i mogućnošću povezivanja sa e-tržištima (*eBay*), alatima za marketing i odnose s kupcima i sopstvenim softverom za izgradnju, koji je jednostavan za upotrebu.
- *Shopsite* je jedan od najkompletnijih alata niže klase za kreiranje sajta e-prodaje, koji pruža sve važne funkcije neophodne za kreiranje, pokretanje i praćenje rada sajta e-trgovine.
- *Merchandizer* je softver zasnovan na korpi za kupovinu, čije se sve funkcije realizuju na Web severu, tako da nije potrebna nikakva softverska instalacija.

Slika 4.12 – Prikaz nekih funkcija softverskog paketa e-trgovine kompanije Yahoo

4.2.8 Izbor softverskog paketa e-trgovine

Izbor odgovarajućeg paketa e-trgovine jedan je od najtežih zadataka u izgradnji Web sajta e-trgovine. Potrebno je upoznati i oceniti različite karakteristike ponuđenih paketa, kao i skrivene troškove u vidu obuke i organizacionih promena, koje uvođenje zaokružnog paketa može da zehteva.

Prilikom izbora odgovarajućeg paketa, treba razmotriti sledeće faktore:

- Funkcije, opšte i posebne, kao što je podrška za audio i video u realnom vremenu;
- Podršku za različite poslovne modele;
- Alate za modelovanje poslovnih procesa;
- Alate za vizuelni menadžment sajta i kreiranje izveštaja;
- Performanse i mogućnost proširenja;
- Sposobnost povezivanja sa postojećim poslovnim sistemima;
- Usaglašenost sa standradima;
- Globalnu i multikulturnu podršku (jezici, pisma, valute);
- Podrška za primenu globalnih i lokalnih propisa, kao što su porezi i pravila isporuke.

4.3. IZBOR HARDVERA ZA WEB SAJT E-TRGOVINE

Kompjuterska opreme koju koristi sistem da bi realizovao svoje funkcije u e-trgovini se često naziva *hardverska platforma*.

Posebno svojstvo Web sistema je da server ne mora da održava stalnu interakciju sa klijentom i ne pamti stanje klijenta između komunikacije (*stateless*).

Važno svojsvo aplikacije je odnos upotrebe procesora i ulazno-izlaznih uređaja u normalnom radu. Kada aplikacija više koristi ulazno-izlazne (*input/output*) operacije nego standardna računarska obrada, naziva se *I/O Intensive*, a kada zahteva veliku procesnu snagu, naziva se *CPU Intensive*.

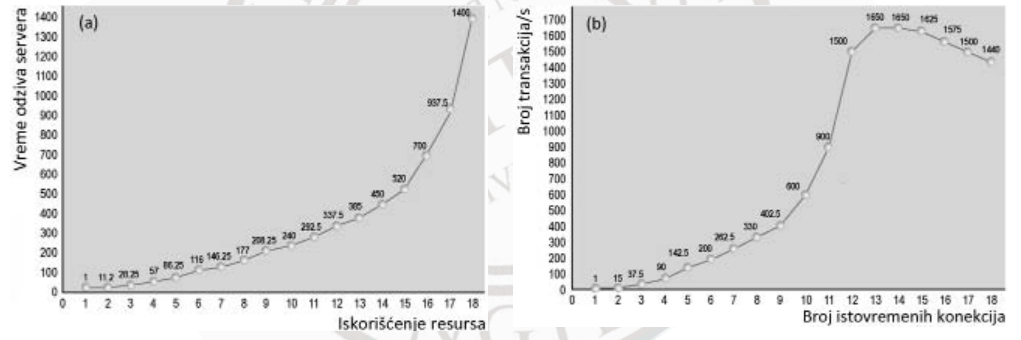
Računari se konfigurišu tako da zadovolje postavljene zahteve za obe kategorije operacija u najlošijem slučaju.

Dimenzionisanje hardverske konfiguracije

Osnovni faktor ispravnog dimenzionisanja performansi i kapaciteta hardvera i softvera su potrebe korisnika Web sajta, koje je teško kvantifikovati. Potrebno je razmotriti [1]: vrstu sadržaja, potreban nivo bezbednosti, način pretraživanja, broj različitih proizvoda (unique items/stock keeping units, SKUs), obim i intenzitet transakcija, složenost integracije s postojećim aplikacijama i procenjeni broj posetilaca ili istovremenih korisnika (page views/hits).

Najvažniji faktor opterećenja je broj istovremenih korisnika, koji u jednoj sesiji (obraćanju) zahtevaju neku stranicu i sačekaju odgovor, nakon čega se sesija okončava. Vreme odgovora servera zavisi od složnosti zahteva, brzine servera i broja istovremenih zahteva.

Na slici 4.13 prikazan je pad performansi, koji nastaje povećanjem broja istovremenih korisnika: (a) porast iskorišćenja resursa (procesori, diskovi i slično) linearan je do tačke preopterećenja, nakon čega raste nelinearno i (b) broj transakcija u jedinici vremena raste do tačke preopterećenja servera, kada dalji porast broja korisnika nije moguć, a vreme odziva servera se povećava zbog dodatnih zadataka, sve do mogućeg otkaza.



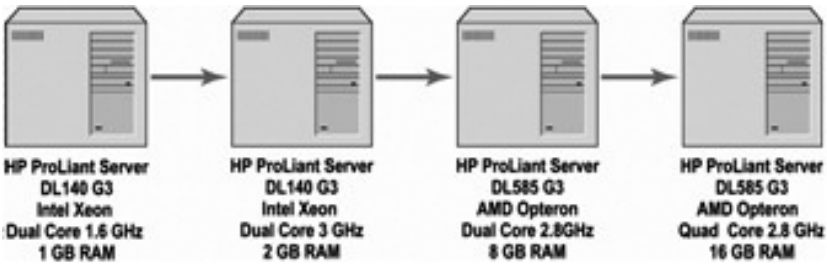
Slika 4.13 Iskorišćenje resursa i vreme odziva u odnosu na brojem istovremenih korisnika

Drugi važan faktor ponašanje korisnika na Web sajtu i vrsta zahteva. Istraživanja su pokazala da 3/4 korisnika sajtova e-trgovine samo pregleda sadržaj, odnosno od servera zahteva samo statičke stranice malog obima [1]. Složeniji zahtevi su pretraživanje sajta i kupovina, koji zahtevaju značajnije angažovanje serverskih procesora i višestruko smanjuju ukupne performanse sistema.

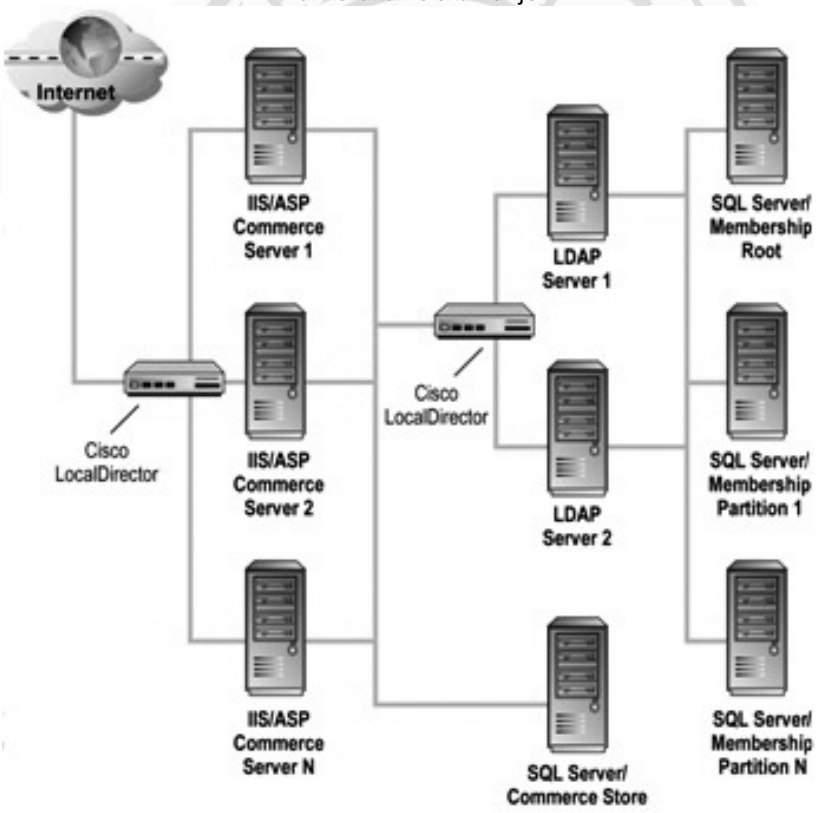
Treći važan faktor je određivanje brzine Internet komunkacije (bandwidth), koja omogućava da planirani broj istovremenih korisnika pristupi sajtu. Npr. širokopojasna DSL linija brzine 2Mb/s omogućava približno 200 istovremenih korisnika, pod uslovom da zahtevaju stranice ili fajlove prosečnog obima 1KB (2Mb/s≈200KB/s).

Izbor i nabavka hardverske konfiguracije

Definisanje osnovnih zahteva za performansama omogućava pravilan izbor nove ili nadogradnju (scaling) postojeće hardverske konfiguracije servera. Nadogradnja može biti vertikalna (povećanje performansi postojećih komponenti) ili horizontalna (povećanje performansi umnožavanjem komponenti), Slika 4.14.



a. vertikalno skaliranje



b. horizontalno skaliranje

Slika 4.14 Tehnike skaliranja hardverske konfiguracije

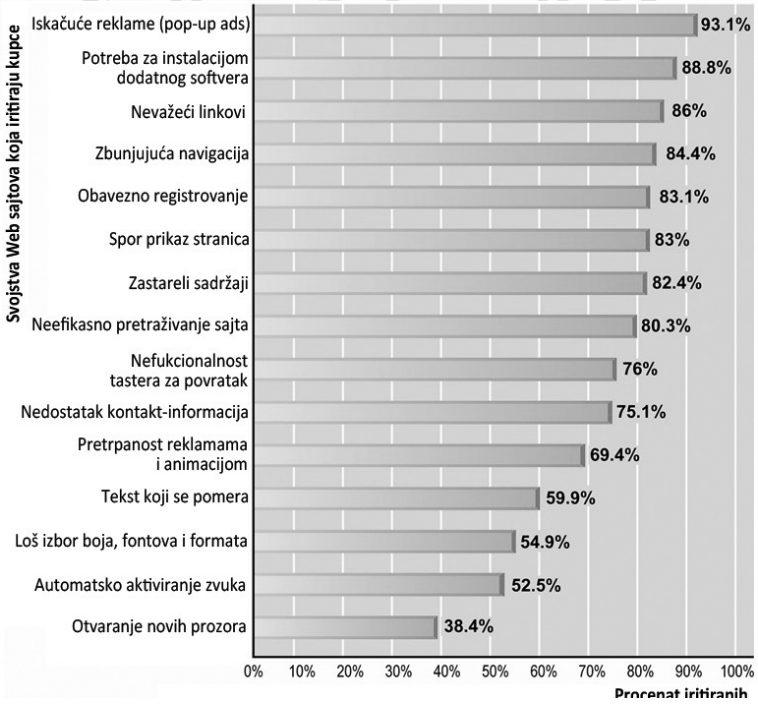
Vertikalna nadogradnja može biti skupa i osetljiva na stanje ispravnosti malog broja skupih komponenti. Horizontalna nadogradnja se zasniva na jeftinijim komponentama i uvodi redundansu, koja omogućava normalan rad u slučaju otkaza dela komponenti, ali zahteva dodatni softver za raspodelu i balansiranje opterećenja pojedinih komponenti (load balancing).

Moguć je i treći pristup, istovremeno horizontalno i vertikalno skaliranje, odnosno nadogradnja sistema.

4.4. OSTALI SOFTVERSKI ALATI WEB SAJTA E-TRGOVINE

Osim izgradnje funkcionalnog Web sajta dobrih tehničkih performansi, za uspeh e-trgovine neophodno je ispunjenje i određenih poslovnih zahteva, kao što je praćenje ponašanja kupaca i personalizacija, čime se kupcu omogućava brže i laksše pronalaženje i kupovina proizvoda.

Koristan pristup je analiza nedostataka koji najviše ometaju proces kupovine, odnosno iritiraju posetioce sajtova e-trgovine, Slika 4.15.



Slika 4.15 Osobine Web sajta e-trgovine koje najviše iritiraju posetioce

Svojstva dobrog dizajna i uspešnosti Web sajta e-trgovine su: funkcionalnost, informativnost, jednostavnost korišćenja, redundantna navigacija, jednostavnost realizacije kupovine, kompatibilnost sa različitim Web čitačima, jednostavna i diskretna grafika i zvuk i dobra čitljivost teksta.

Softver koji omogućava postizanje dobrih svojstava Web sajta e-trgovine obuhvata niz softverskih tehnologija za postizanje visokog stepena interaktivnosti Web sajta.

Opšti programski interfejs (Common Gateway Interface, CGI)

Skup standarda za komunikciju Web čitača i programa koji se izvršavanju na Web serveru, npr. programa korpe za kupovinu. Ovi CGI programi su u obliku izvšnog mašinskog koda, pa mogu biti napisani u bilo kom programskom jeziku.

Tehnologija ASP (Active Server Pages)

Prvi programski jezik za kreiranje dinamičkih stranica je *JavaScript* (originalni naziv *LiveScript*), koji ima posebne podverzije za serversku i klijentsku stranu. Po ugledu na jezik C++ kreirala ga je kompanija *Netscape*, jedna od prvih kompanija za proizvodnju komercijalnog Web softvera.

Jezik *JavaSript* je standardizovan u Evropi kao *ECMA Script*. Kompanija *Microsoft* je izradila svoju verziju jezika i nazvala ga *JScript*, ali je za programere koji su poznavali jezik Visual Basic kreirala novi, pod nazivom *VBScript*, koji je takođe namenjen programiranju dinamičkih HTML stranica, posebno radi pristupa podacima u bazama podataka. Kompletna tehnologija izrade dinamičkih stranica, odnosno Web aplikacija, dobila je naziv *Active Server Pages* (ASP).

Vremenom su različiti proizvođači softvera kreirali svoje serverske jezike (*VBScript*, *PHP*, *C#*), ali je *JavaScript* ostao standardni klijentski jezik, koga podržavaju svi *Web* čitači i koji olakšava programiranje *Web* strana neprofesionalcima, jer je lakši za razumevanje od jezika *Java*.

Tehnologija Java i Java Server Pages (JSP)

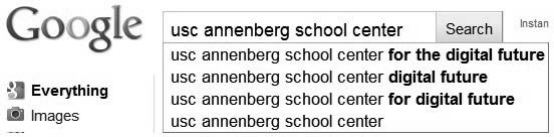
Java je programski jezik za pisanje programa za elektronske uređaje koji ne zavise od hadverske platforma (vrste procesora ili operativnog sistema). Java programi (Java applets) se mogu preuzeti putem mreže u izvornom obliku i izvršiti na bilo kojem uređaju koji ima instaliran Java interpreter (virtuelnu mašinu, VM), npr. mobilnom telefonu.

Komponente ActiveX i jezik VBScript

Kompanija Microsoft je razvila sopstvene tehnologije za izradu Web aplikacija, između ostalog ActiveX i jezik VBSript. Interaktivne kontrole tehnologije ActiveX su bile alternativa Java apletima, a jezik VBScript konkurencija jeziku JavaSript.

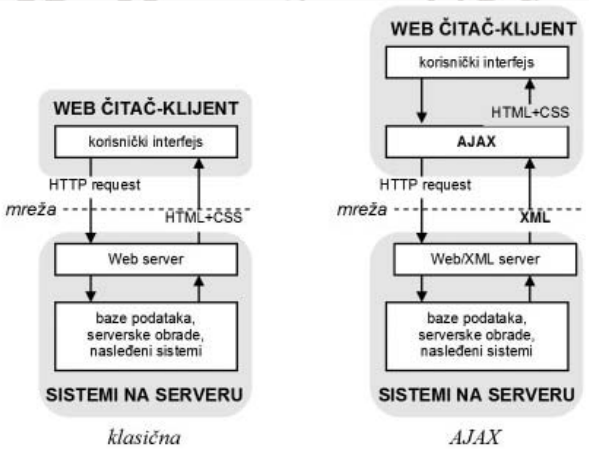
Ilustracija: Obogaćivanje korisničkog iskustva preko AJAX i Flash tehnologije

Skraćenica AJAX potiče od *Asynchronous JavaScript and XML*. Asinhroni način rada odnosi se na mogućnost izmene delova Web stranice bez kopiranja i osvežavanja prikaza kompletne stranice, što omogućava bržu reakciju na događaje koji nastaju u interakciji s korisnikom. Pretraživač *Google* koristi ovu tehnologiju za vreme unosa upita u obliku predloga varijanti smislene formulacije upita, Slika 4.16.



Slika 4.16 Primena AJAX tehnologije u pretraživaču Google

Osim toga, predviđen je i rad sa XML dokumenatima. Na slici 4.17 prikazana je razlika u funkcionisanju klasične i AJAX Web aplikacije [8].



Slika 4.17 - Promena modela komunikacije klijenta i servera u AJAX tehnologiji

AJAX predstavlja posebnu kombinaciju više različitih Web tehnologija:

- prikaz podataka zasniva se na jezicima XHTML i CSS
- dinamički prikaz i interakcija realizuju se korišćenjem Document Object Model-a
- razmena i manipulacija podacima vrši se korišćenjem jezika XML i XSLT
- asinhroni pristup podacima se realizuje upotrebom XMLHttpRequest
- integracija tehnologija se vrši pomoću jezika JavaScript.

Tehnologija ColdFusion

Još jedna tehnologija programiranja serverskih Web aplikacija uz pomoć posebnog jezika CFML (Could Fusion Markap Language), koju je razvila kompanija Macromedia.

Alati za personalizaciju

Personalizacija je sposobnost sistema da tretira posetioce na osnovu njihovih ličnih osobina i istorije aktivnosti na Web sajtu. Kastomizacija (customization) je sposobnost prilagođavanja potrebama korisnika.

Osnovni alat za obezbeđenje personalizacije su kolačići, zapisi u tekstualni fajlovima, koje Web server ostavlja na klijentskim računarima. U tim zapisima različiti programi beleže podatke o posetama i drugim aktivnostima korisnika na određenom Web sajtu. Programi koriste ove podatke za formiranje istorije ponašanja, odnosno personalizacije ponude i proizvoda.

Politika upravljanja informacijama (Information Policy Set)

Razvoj Web sajta e-trgovine podrazumeva i definisanje politike obezbeđenja privatnosti podataka, ore svega o kupcima, koja se objavljuje u vidu javne izjave na samom sajtu e-trgovine.

Projektovanje dostupnosti

Dostupnost je važna osobina javnog Web sajta, skup tehnoloških rešenja kojima se obezbeđuje pristup i ravnopravna upotreba sajta e-trgovine i za lica sa posebnim potrebama.

Postoje tri nivoa dostupnosti, odnosno zahteva:

1. Zahtevi koji se obavezno moraju zadovoljiti, jer obezbeđuju dostupnost Web dokumenata svim kategorijama korisnika (omogućavanje pristupa);
2. Zahtevi koje treba zadovoljiti, jer sprečavaju teškoće koje će u pristupu Web dokumentima imati jedna ili više kategorija korisnika (uklanjanje značajnih prepreka);
3. Zahtevi koji se mogu zadovoljiti, pošto sprečavaju neke teškoće koje jedna ili više kategorija korisnika mogu imati u pristupu Web dokumentima (unapređenje pristupa).

Za postizanje dostupnosti se koristi multimedijska komunikacija (tekst, zvuk, video, dodir), odnosno više različitih načina komunikacije kojima se obezbeđuje korišćenja Web sajta od strane lica sa posebnim potrebama.

Proveru dostupnosti treba vršiti već u ranim fazama razvoja Web sajta, jer je tada lakše izbeći greške i izvršiti eventualne ispravke.

Validacija dostupnosti se može izvršiti automatizovano i pregledom od strane čoveka. Automatizovane metode su brže, ali ne mogu da otkriju sve moguće probleme.

Ilustracija: Web sajt za prodaju planinarske opreme kompanije REI

Proces razvoja uspešnog Web sajta e-trgovine ilustrovaće se na primeru kompanije za prodaju planinarske opreme *Recreational Equipment, Inc. (REI)* [1]. Kompanija *REI* osnovana je 1938. godine. Vlasnici, i sami planinari, počeli su posao nakon iskustva sa nabavkom planinarske opreme iz Austrije za lične potrebe. Razvili su maloprodaju kvalitetne planinarske opreme, sa prodavnicama u 24 države SAD, online prodajom i trurističkom agencijom, ukupno preko 6.000 zaposlenih.

Menadžment kompanije se zainteresovao za mogućnosti Web-a još u prvoj fazi razvoja e-trgovine. Dok su se tadašnji prodavci plašili pada prodaje u svojim maloprodajnim objektima zbog uvođenja online prodaje, predsednik kompanije REI je smatrao da će se kupci koji žele da kupuju online jednostavno kupovati kod drugih prodavaca, koji ponude takav način kupovine. Kasnije se okazalo se da mogućnost online kupovine koriste kupci koji kupuju i na klasičan način, te da oni ukupno kupuju znatno više.

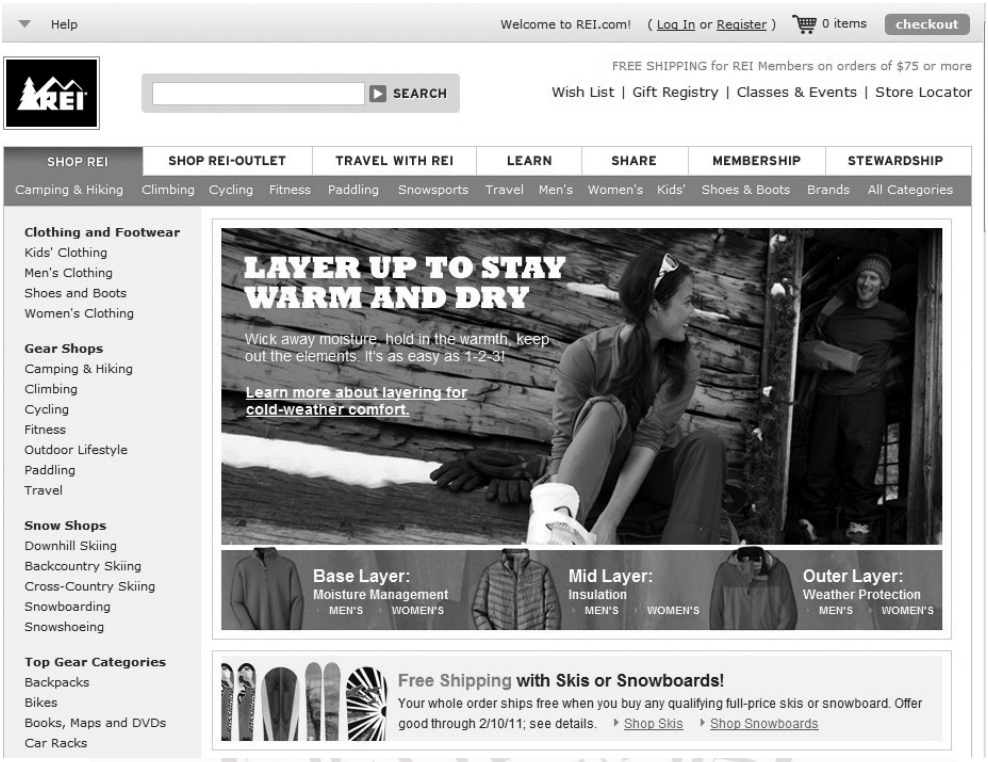
Kompanija se odlučila za nabavku softverskog paketa za e-trgovinu i odlučila se za *Netscape Merchant Server*, jedino kompletno rešenje u to vreme. Softver je instaliran na tada veoma savremen server IBM RS/6000.

Odluka o nabavci paketa donesena je s obrazloženjem da kompanija neće prodavati softver. S druge strane, razvoj sajta je izvršen u sopstvenoj režiji (*in-house*), jer se smatralo da se to ne može prepuštati drugima. To je zahtevalo zapošljavanje novih kadrova, kojih je bilo znatno manje nego u maloprodaji, ali su njihove plate bile višestruko veće.

Sajt *rei.com* je prvu porudžbinu dobio 20 minuta nakon postavljanja i prodaja je počela da raste. Kada je broj kupaca sa nekoliko hiljada mesečno narastao na milion, pojavio se problem performansi usvojenog rešenja, koje se nije moglo jednostavno unaprediti. Menadžment je tražio rešenje koje će zadovoljiti zahteve u dužem vremenskom periodu i odlučuio se za *IBM Net.Commerce* serverski softver.

Izrađen je i pokrenut novi sajt *re-outlet.com*, a originalni je preseljen na novu tehnološku platformu 1998. godine. Sledeća prilika za reviziju rešenja nastupila je 2002. godine, nakon odluke da se, radi smanjenja dugoročnih troškova, dalji razvoj softverskih rešenja veže za jednog proizvođača integrisanih rešenja softvera e-trgovine. Izabrana je integrisana platforma za *razvoj* softvera *IBM WebSphere* i odgovarajući skup softverskih rešenja kompanije IBM, zasnovanih jeziku *Java*, operativnom sitemu *Unix* i multiprocesorskim sistemima firme IBM.

Današnji Web site *rei.com* nudi veći broj proizvoda nego bilo koja fizička prodavnica, ima 45.000 stranica informacija o proizvodima i sistem za interaktivno povezivanje, Slika 4.18. Softversko rešenje kompanije je nagrađivano kao inovativno i ocenjeno kao jedno od najboljih po doživljaju klijenata i integraciji tehnologija.



Slika 4.18 Sadašnji izgled Web sajta kompanije REI

Dalji razvoj sajta je usmeren na personalizaciju i odnos s klijentima, što npr. omogućava da se novim Web korisnicima preporuče ili ponude pogodnosti kupovine u obližnjim prodavnicama i tako pomoću onlajn prodaje pospeši prodaja realnih prodavnica. Takođe je izuzetno uspela ponuda besplatne dostave online kupcima, koja se vrši periodično, vozilma redovnog snabdevanja prodavnica. Uvođenje ove mogućnosti dovelo je do povećanja online prodaje, jer korisnici ove usluge zbog toga kupuju više robe.

Poslovanje kompanije je u stalnom usponu, tako da je 13 uzastopnih godina na spisku 100 najuspešnijih kompanija magazina Fortune. Obim prodaje je u 2009. godini bio 1,43 milijarde dolara, dok se neto prihod od 2002. godine povećao sa 16 na 29,8 miliona dolara [rei.com].

4.5. LITERATURA

[1] Laudon K.C., Traver C.G., *E-commerce, business, technology, society*, 3rd Ed, Addison Wesley, 2006

[2] Whitten J. L., Bentley L. D., Dittman K. C., *Systems Analysis and Design Methods*, 7th Ed, Irwin McGraw Hill, 2007.

[3] Hoffer J.A., George J.F., Valacich J.S., *Modern Systems Analysis And Design*, 4th Ed, Pearson-Prentice-Hall Inc., 2005.

[4] Lynch P. J., Horton S., *Web Style Guide: Basic Design Principles for Creating Web Sites*, 3rd Ed, Yale University, 2009 http://www.webstyleguide.com

[5] Vidgen R., Avison D., Wood B., Wood-Harper T., *Developing Web Information Systems*, Butterworth Heinemann, 2003.

[6] www.webtrends.com

[7] Tyler M. E., Ledford J., *Google Analytics*, Wiley Publishing, Inc, 2006

[8] Miškovic V., *Multimedija – praktikum za laboratorijske vežbe*, Univerzitet Singidunum, Beograd, 2008

[9] http://shopping-cart-review.toptenreviews.com

[10] Quin Z., *Introduction to E-commerce*, Springer, 2009

[11] Kurbel K. E., *The Making of Information Systems*, Springer-Verlag, 2008

[12] Niederst R. J., *Learning Web Design*, O'Reilly Media, Inc, 2007

[13] Sarkar S., *Joomla! E-Commerce with VirtueMart*, Packt Publishing, 2009

[14] Loshin P., Vacca J., *Electronic Commerce*, 4thEd, Barnes and Noble, 2003

[15] www.whatis.com

[16] http://www.useit.com/alertbox/991003.html

[17] www.marketingterms.com

[18] www.merriam-webster.com

[19] www.wikipedia.org

[20] www.internet2.edu

[21] www.freewebstore.org

[22] www.rei.com

5. BEZBEDNOST ELEKTRONSKE TRGOVINE

5.1 UOPŠTE O BEZBEDNOSTI

Elektronska trgovina smanuje troškove i olakšava poslovanje. Ipak, postoje i potencijalni rizici upotrebe ove tehnologije. Na primer, elektronska infrastruktura je osetljiva na različite oblike napada. Procenat transakcija na Internetu u kojima je došlo do povrata novca je veći nego u uobičajenoj trgovini – od 3% do 5% za online trgovinu prema 0, 5% do 1% za tradicionalan način kupovine, zaključak je na osnovu industrijskih procena. Celinu problema teško je utvrditi jer velike kompanije ne žele da objave prave cifre. Internet pospešuje globalnu trgovinu, tako da će se i broj prevara u budućem razvoju e-trgovine povećati, uporedo sa rastom Interneta. Sa ekonomske tačke gledišta, posledice otkaza tehnološke prirode ili zloupotrebe ove tehnologije od strane korisnika mogu biti sledeće:

- Direktni finansijski gubici kao posledica prevare – Zlonamerna osoba može, na primer, da prebaci izvesnu količinu novca sa jednog računa na drugi ili može da obriše podatke finansijske prirode.
- Gubljenje vrednih i poverljivih informacija – Mnoga preduzeća memorišu i šalju informacije tehnološke prirode ili podatke o svojim kupcima i dobavljačima, čija poverljivost je od najveće važnosti za njihovo poslovanje. Ilegalan pristup takvim informacijama može prouzrokovati značajne finansijske gubitke ili štete druge vrste takvom preduzeću.
- Gubljenje poslova zbog nedostupnosti servisa – Elektronski servisi mogu biti nedostupni u dužem vremenskom periodu ili u periodu značajnom za obavljanje konkretnog posla, zbog napada na sistem od strane zlonamernih osoba ili zbog slučajnih otkaza sistema. Posledice takvih događaja (finansijske prirode ili druge vrste) mogu biti katastrofalne za jedno preduzeće.

- Neovlašćena upotreba resursa – Napadač koji ne pripada organizaciji koju napada može neovlašćeno pristupiti nekim resursima njenog računarskog sistema i upotrebiti ih radi pribavljanja imovinske koristi. Tipičan primer resursa osetljivog na takvu vrstu napada je telekomunikacioni servis. ''Krakeri'' često koriste računar kome su neovlašćeno pristupili kako bi napali ostale računare u mreži.
- Gubljenje poslovnog ugleda i poverenja klijenata – Preduzeće može pretrpeti značajne gubitke zbog lošeg iskustva svojih klijenata ili zbog negativnog publiciteta koji mogu biti posledica napada na njegov servis elektronske trgovine, ili ponašanja zlonamerne osobe koja se predstavlja kao pripadnik tog preduzeća.
- Troškovi izazvani neizvesnim uslovima poslovanja – Česti prekidi funkcionisanja servisa izazvani napadima spolja ili iznutra, greškama i sl. mogu paralisati izvršenje poslovnih transakcija u značajnom vremenskom periodu. Na primer, potvrde transakcija koje ne mogu da se prenesu komunikacionim kanalima, transakcije koje mogu biti blokirane od strane trećih lica itd. Finansijski gubici koje ovakvi uslovi poslovanja mogu izazvati mogu biti značajni.

Teško je proceniti tačan broj i finansijske posledice kriminalnih radnji vezanih za e-trgovinu. U velikom broju slučajeva bezbednosni incidenti se ne prijavljuju jer se kompanije boje da će izgubiti poverenje kupaca. Nedavno istraživanje sprovedeno od strane Computer Security Institute je pokazalo da od 538 korporacija i vladinih organizacija u SAD-u koje koriste zaštitne mere njih 85% je otkrilo neovlašćeni prodor u računarske sisteme zaštite u poslednjih 12 meseci, a 64% je priznalo da j zbog toga imalo novčane gubitke. Međutim samo 35% je bilo voljno da brojčano izrazi finansijske gubitke koji su ukupno iznosili $377 miliona. Najozbiljniji gubici su uključivali krađu vlasničkih informacija i novčane prevare. Četrdeset procenata prijavljenih upada su izvedeni izvan organizacionih okvira, 38% otpada na napade zvane uskraćivanje usluga (Denial of Service - DOS) i 94% je prijavilo napade virusa [1].

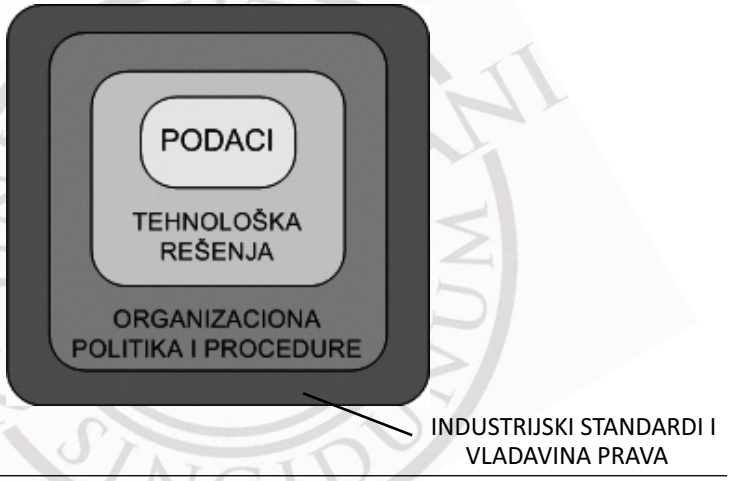
Smanjenje rizika u e-trgovini je kompleksan proces koji uključuje nove tehnologije, organizacionu politiku i procedure kao i zakone i industrijske standarde koji će omogućiti da sprovodioci zakona istražuju i procesuiraju prestupnike. Sl.5.1 prikazuje višeslojnost zaštite elektronske trgovine.

Da bi se postgao najviši stepen zaštite potrebno je koristiti nove dostupne tehnologije. Ali samo tehnologije neće rešiti problem. Organizaciona politika i procedure su potrebne da bi se osiguralo da tehnologija ne bude zloupotrebljena. Industrijski standardi i zakoni na nivou države su potrebni da se ojačaju platni mehanizmi kao i da se pronađu i procesuiraju prekršitelji zakona osmišljenog da štiti transfer vlasništva u trgovinskim transakcijama.

Praksa zaštite trgovinskih transakcija pokazuje da se svaki sistem zaštite može probiti ako se angažuje dovoljno sredstava. Apsolutnu zaštitu je teško postići i ona bi bila izuzetno skupa. Na sreću, apsolutna zaštita nije ni potrebna kada je reč o komercijalnim transakcijama. Postoji vremenska aktuelnost informacija isto kao što postoji vremenska

vrednost novca. Ponekad je dovoljno zaštititi informaciju na nekoliko sati, dana ili godina. Budući da je sistem zaštite skup, izabrani nivo zaštite mora biti kompromis između stvarnih potreba i troškova koje jedna kompanija može da podnese. Ne treba gubiti iz vida da je po svojoj prirodi lanac mera zaštite snažan koliko i njegova najslabija karika. Stoga većeg smisla ima napor na ujednačenim i međsobno usaglašenim merama zaštite od skupih pojedinačnih mera u okruženju slabih ostalih mera zaštite.

Možemo zaključiti da sigurna elektronska trgovina zahteva skup zakona, procedura, politika i tehnoloških mera [2]. U tehnološke mere spadaju, između ostalog, neporecivost, autentikacija, poverljivost i integritet podataka. Da bi se ove mere sprovele u praksi, neophodna je upotreba kriptoloških tehnologija, kao na primer digitalni potpis i šifarski sistemi sa javnim ključem. Jedan od ciljeva poglavlja je i detaljnije upoznavanje sa ovim savremenim bazičnim tehnikama zaštite informacija, na kojima se zasniva bezbednost savremenog elektronskog poslovanja.



Sl.5.1 Višeslojno zaštitno okruženje e-trgovine. Lanac bezbednosti je jak koliko je jaka njegova najslabija karika.

Na kraju, bezbedna elektronska trgovina se može definisati kao elektronska trgovina kod koje se koriste bezbednosne procedure u skladu sa procenjenim rizicima.

Osnovni ciljevi mera bezbednosti u informacionim sistemima su:

- Poverljivost – obezbeđuje nedostupnost informacija neovlašćenim licima.
- Integritet – obezbeđuje konzistentnost podataka, sprečavajući neovlašćeno generisanje, promenu i uništenje podataka.
- Dostupnost – obezbeđuje da ovlašćeni korisnici uvek mogu da koriste servise i da pristupe informacijama.
- Upotreba sistema isključivo od strane ovlašćenih korisnika – obezbeđuje da se resursi sistema ne mogu koristiti od strane neovlašćenih osoba niti na neovlašćen način.

Glavne naučne discipline čiji rezultati se koriste da bi se ostvarili pomenuti ciljevi su nauka o bezbednosti komunikacija i nauka o bezbednosti u računarima. Bezbednost komunikacija označava zaštitu informacija u toku prenosa iz jednog elektronskog sistema u drugi. Bezbednost u računarima označava zaštitu informacija unutar računarskog sistema – ona obuhvata bezbednost operativnog sistema i aplikativnog softvera, naročito softvera za manipulisanje bazama podataka. Mere bezbednosti komunikacija i bezbednosti u računarima se kombinuju sa drugim merama (fizičko obezbeđenje, bezbednost personala, bezbednost administracije, bezbednost medija) radi ostvarenja pomenutih ciljeva.

Potencijalne pretnje jednom informacionom sistemu koji sadrži podsistem za elektronsku trgovinu su:

- Infiltracija u sistem – Neovlašćena osoba pristupa sistemu i u stanju je da modifikuje datoteke, otkriva poverljive informacije i koristi resurse sistema na nelegitiman način. U opštem slučaju, infiltracija se realizuje tako što se napadač predstavlja sistemu kao ovlašćeni korisnik ili korišćenjem slabosti sistema (npr. mogućnost izbegavanja provere identiteta i sl.). Informacije neophodne za infiltriranje napadač dobija koristeći neku drugu vrstu napada. Primeri takvih napada su "dumpster diving attack", kod koga napadač dobija potrebnu informaciju pretražujući materijal koji žrtva smatra suvišnim, i "socijalni inženjering" kod koga napadač dobija neophodne informacije primoravajući na neki način (ucena, pretnja i sl.) svoju žrtvu da mu ih da.
- Prekoračenje ovlašćenja – Lice ovlašćeno za korišćenje sistema koristi ga na ne-ovlašćeni način. To je vrsta pretnje koju ostvaruju kako napadači iznutra ("insiders") tako i napadači spolja. Napadači iznutra mogu da zloupotrebljavaju sistem radi sticanja koristi bilo koje vrste. Napadači spolja mogu da se infiltriraju u sistem predstavljajući se kao korisnici sa manjim ovlašćenjima i nastaviti sa infiltriranjem u sistem koristeći takav pristup radi neovlašćenog proširenja korisničkih prava.
- Suplantacija – Obično posle uspešnog infiltriranja u sistem, napadač ostavlja u njemu neki program koji će mu omogućiti da olakša napade u budućnosti. Primer suplantacije je upotreba "trojanskog konja" – to je softver koji se korisniku predstavlja kao normalan, ali koji prilikom izvršenja otkriva poverljive informacije napadaču ili na drugi način deluje štetno na sistem. Na primer, tekst procesor može da kopira sve što ovlašćeni korisnik unese u jednu tajnu datoteku kojoj može da pristupi napadač.
- Prisluškivanje – Napadač može da pristupi poverljivim informacijama (npr. lozinci za pristup sistemu) prostim prisluškivanjem protoka informacija u komunikacionoj mreži. Postoje specijalizovani programi opšte namene ("packet sniffers") za analizu protokola koji se koriste na komunikacionoj liniji (najčešće se radi o http ili smtp protokolu). Informacija dobijena na ovaj način može se iskoristiti radi olakšavanja drugih vrsta napada.

- Promena podataka na komunikacionoj liniji – Napadač može da promeni informacije koje se prenose kroz komunikacionu mrežu. Na primer, on može namerno da menja podatke finansijske prirode za vreme njihovog prenošenja kroz komunikacioni kanal ili da se predstavi kao ovlašćeni server koji od ovlašćenog korisnika zahteva poverljivu informaciju.
- Odbijanje servisa – Zbog čestih zahteva za izvršenje složenih zadataka izdatih od strane neovlašćenih korisnika sistema, servisi sistema mogu postati nedostupni ovlašćenim korisnicima.
- Poricanje transakcije – Posle izvršene transakcije, jedna od strana može da poriče da se transakcija dogodila. Iako ovakav događaj može da nastupi usled greške, on uvek proizvodi konflikte koji se ne mogu lako rešiti.

5.2 BEZBEDNOSNI SERVISI

Rukovodstvo organizacije u kojoj postoji komunikaciona mreža i/ili računari obično uspostavlja jedan skup pravila koja se odnose na sve aktivnosti te organizacije u vezi sa bezbednošću. Ovaj skup pravila se naziva *politika bezbednosti* [3]. Politika bezbednosti se sprovodi u praksi putem *bezbednosnih servisa* [4].

Bezbednosni servisi su delovi sistema koji realizuju aktivnosti koje pariraju pretnjama vezanim za bezbednost sistema. Zbog značajnih računarskih resursa koji su potrebni za njihovo adekvatno funkcionisanje, oni obično nisu stalno uključeni, već deluju na zahtev. Postoji šest osnovnih vrsta bezbednosnih servisa:

Servis poverljivosti. Ovaj servis sprečava otkrivanje informacije bilo kom entitetu (licu ili organizaciji) koji za to nema ovlašćenje. Poverljivost se ostvaruje upotrebom šifre. Međutim, deo informacija koje mogu biti od značaja može se dobiti i na drugi način. Na primer, moguće je posmatrati broj i veličinu poruka koje se šalju na određenu adresu svakog dana, bez uvida u njihov sadržaj.

Servis integriteta. Ovaj servis štiti informaciju od promena koje nisu dozvoljene politikom bezbednosti. U takve promene spada umetanje dodatnih podataka, brisanje, supstitucija ili preuređenje podataka.

Servis autentikacije. Ovaj servis obezbeđuje garanciju identiteta. To znači da kada neki entitet daje neki podatak o svom identitetu (kao na primer ime), servis autentikacije proverava vrednost tog podatka. Znači, autentikacija je sredstvo protiv infiltriranja u sistem. Postoje dve osnovne varijante servisa autentikacije: (1) autentikacija entiteta, koja proverava identitet predstavljen od strane udaljenog korisnika (lozinke predstavljaju opšte poznati mehanizam autentikacije entiteta) i (2) autentikacija porekla podataka, koja proverava identitet pošiljaoca podataka, na primer neke poruke (ovo se ostvaruje proverom digitalnog potpisa).

Servis kontrole pristupa. Ovaj servis štiti sistem od neovlašćenog pristupa pojedinim njegovim resursima (podsistem za izvršenje proračuna, komunikacioni podsistem, memorija itd.). Termin neovlašćeni pristup obuhvata upotrebu, otkrivanje, modifikaciju, destrukciju podataka, kao i izvršenje aplikacija bez ovlašćenja. Kontrola pristupa je osnovna mera za izvršenje autorizacije, tj. za definisanje prava pristupa resursima sistema od strane *ovlašćenih korisnika*.

Servis neporecivosti - Servis za onemogućavanje poricanja transakcije. Ovaj servis štiti od nastupanja događaja kada jedna od strana učesnica u transakciji poriče da se transakcija dogodila. Ovaj servis je suštinski različit od ostalih bezbednosnih servisa. Njegova osnovna namena je da zaštiti ovlašćene korisnike sistema od drugih ovlašćenih korisnika, a ne od napadača. Ovaj servis, međutim, ne može da spreči poricanje transakcije. Naprotiv, on obezbeđuje jedan pouzdan dokaz koji se može upotrebiti u slučaju konflikta između strana učesnica u transakciji. Drugi razlog za postojanje ovog servisa je mogućnost nastupanja slučajne greške za vreme izvršenja transakcije posle koje svaka od strana učesnica na različit način ocenjuje njenu realizaciju.

Servis za onemogućavanje odbijanja usluge. Napad koji prouzrokuje odbijanje usluge nastaje onda kada zlonamerna osoba podnese takav skup uzastopnih zahteva serveru koji onemogućava njihovo izvršenje. Na taj način, server ne može da odgovori ni na legalne zahteve. Pomenuti servis ograničava upotrebu resursa servera, kao na primer vreme izvršenja CPU-a, količinu memorije koja se koristi, broj otvorenih datoteka ili broj istovremeno aktivnih procesa.

U Tabeli 5.1 sumirane su najvažnije dimenzije zaštite e-trgovine iz perspektive kupca i prodavca.

Tabela 5.1 Različite dimenzije zaštite e-trgovine iz perspektive kupca i prodavca

DIMENZIJE	PERSPEKTIVA POTROŠAČA	PERSPEKTIVA TRGOVCA
Integritet	Da li je informacija koju sam poslao ili primio izmenjena?	Da li su podaci izmenjeni bez odobrenja? Da li su tačni podaci dobijeni od kupca?
Neporecivost	Da li druga strana može kasnije da negira obavljenu poslovnu transakciju?	Da li kupac može kasnije negirati narudžbinu?
Autentikacija	Sa kim poslujem? Kako mogu biti siguran da je osoba ili entitet ona za koju se predstavlja?	Da li je to pravi indentitet kupca?
Poverljivost (tajnost)	Da li neko drugi osim onih kojima su namenjene čita moje poruke?	Da li su poruke ili poverljivi podaci dostupni neovlašćenim osobama?
Privatnost	Mogu li da kontrolišem upotrebu ličnih podataka koje sam dostavio trgovcu?	Koja je korist, ako i postoji, od prikupljenih ličnih podataka prilikom neke transakcije e-trgovine? Da li su lični podaci kupca iskorišćeni na nelegalan način?
Raspoloživost	Imam li pristup ovom Web sajtu?	Da li je Web sajt operativan?

5.3 KRIPTOLOŠKE TEHNIKE I VRSTE ALGORITAMA

Šifrovanje i digitalni potpis su kriptološke tehnike koje se koriste u cilju implementiranja servisa bezbednosni. Osnovni samostalni entitet u okviru kriptoloških tehnika se naziva šifarski sistem. Svaki šifarski sistem obuhvata par transformacija podataka, koje se nazivaju šifrovanje i dešifrovanje. Šifrovanje je procedura koja transformiše originalnu informaciju (otvoreni tekst) u šifrovane podatke (šifrat). Obrnut proces, dešifrovanje, rekonstruiše otvoreni tekst na osnovu šifrata [5].

U šifarskoj transformaciji, pored otvorenog teksta, takođe se koristi i jedna nezavisna vrednost koja se naziva ključ šifrovanja. Na sličan način, transformacija za dešifrovanje koristi ključ dešifrovanja. Broj simbola koji predstavljaju ključ (dužina ključa) zavisi od šifarskog sistema.

Šifarski sistem može u informacionom sistemu obezbeđivati servis poverljivosti. U tom slučaju, otvoreni tekst sadrži poverljivu informaciju koja u takvom obliku ne sme da se nalazi na serveru. Ako je šifarski sistem otporan na napade za koje se proceni da mogu nastupiti, šifrat se može poslati putem komunikacione mreže, bez mogućnosti da neovlašćeno lice dođe do poverljive informacije. Kriterijumi kvaliteta jednog šifarskog sistema definišu se imajući u vidu računarske i druge resurse kojima raspolaže potencijalni napadač.

Postoje dve osnovne vrste šifarskih sistema – simetrični sistemi, koji se dalje dele na sekvencijalne šifarske sisteme i blok šifarske sisteme i asimetrični sistemi ili sistemi sa javnim ključevima. Njihove karakteristike su različite i koriste se na različit način u bezbednosnim servisima.

5.3.1 Simetrični sistemi

Kod simetričnih šifarskih sistema ključ šifrovanja je identičan ključu dešifrovanja. Ključ mora da se drži u tajnosti, što znači da pošiljalac i primalac poruke moraju pre slanja poruke da se dogovore o ključu ili da postoji centar za distribuciju ključeva koji ih distribuira korisnicima šifarskog sistema putem sigurnog kanala. Osnovni algoritam šifrovanja koji spada u ovu kategoriju je Vernamova šifra ("*One time pad*"), kod koje se šifrat dobija sabiranjem po modulu 2 binarnih simbola otvorenog teksta i binarnih simbola ključa [6]. Pre šifrovanja, otvoreni tekst napisan koristeći običan alfabet mora da se pretvori u niz binarnih simbola ("*bita*") koristeći odgovarajući kod. U početku se Vernamova šifra koristila u telegrafskim komunikacijama (teleprinterski saobraćaj, telex), gde se koristio međunarodni kod br. 2, sa 5 binarnih simbola za svako slovo otvorenog teksta.

Suma po modulu 2 (simbol za ovu operaciju je $\oplus$) se računa na sledeći način:

$\oplus$	0	1
0	0	1
1	1	0

Na primer, za šifrovanje poruke "come soon":

Otvoreni tekst:	00011	01111	01101	00101	10011	01111	01111	01110
Ključ:	11011	00101	01011	00110	10110	10101	01100	10010
Šifrat:	11000	01010	00110	00011	00101	11010	00011	11100

Da bi se rekonstruisao originalni otvoreni tekst (poruka), ponovo se niz šifrata sabira po modulu 2 sa nizom ključa, pošto sabiranje i oduzimanje po modulu 2 koincidiraju.

U daljem tekstu, za napadača koji želi da rekonstruiše otvoreni tekst bez poznavanja ključa koristićemo naziv kriptoanalitičar. U tom slučaju, uobičajeno je da se šifrat naziva kriptogram.

Claude Shannon je definisao uslove apsolutne tajnosti [5], polazeći od sledećih osnovnih hipoteza:

1. Tajni ključ se koristi samo jednom.
2. Kriptoanalitičar ima pristup jedino kriptogramu.

Šifarski sistem ispunjava uslove apsolutne tajnosti ako je otvoreni tekst X statistički nezavisan od kriptograma Y, što se može matematički izraziti na sledeći način:

$$P(X = x \mid Y = y) = P(X = x),$$

za sve moguće otvorene tekstove

$$x = (x_1, x_2, \ldots, x_M)$$

i sve moguće kriptograme

$$y = (y_1, y_2, \ldots, y_N);$$

drugim rečima, u apsolutno tajnom šifarskom sistemu, verovatnoća da slučajna promenljiva X ima vrednost x jednaka je sa ili bez poznavanja vrednosti slučajne promenljive Y. Zbog toga kriptoanalitičar ne može bolje proceniti vrednost X poznavajući vrednost Y od procene bez njenog poznavanja, nezavisno od raspoloživog vremena i računarskih resursa kojima raspolaže.

Takođe, koristeći pojam entropije iz teorije informacija, Shannon je odredio minimalnu dužinu ključa potrebnu da bi bili ispunjeni uslovi apsolutne tajnosti. Dužina ključa K mora biti najmanje jednaka dužini otvorenog teksta M:

$$K \geq M.$$

U slučaju Vernamove šifre u gornjoj relaciji važi znak jednakosti.

Dokaz apsolutne tajnosti: Razmotrimo, na primer, algoritam šifrovanja kod koga otvoreni tekst, šifrat i ključ uzimaju vrednosti iz *L*-arnog alfabeta $\{0,1,\ldots,L-1\}$ i u kome su dužine ključa *K*, šifrata *N* i otvorenog teksta *M* međusobno jednake, $K = N = M$. U tom slučaju, broj mogućih otvorenih tekstova, šifrata i ključeva je jednak L^M. Pretpostavlja se sledeće: Ključ se bira na slučajan način:

$$P(Z = z) = L^{-M}$$

za svih L^M mogućih vrednosti *z* tajnog ključa.

a) Šifarska transformacija je:

$$Y_i = X_i \oplus Z_i, \ (i = 1,\ldots,M)$$

gde $\oplus$ označava sabiranje po modulu *L*, simbol po simbol.

b) Za fiksni otvoreni tekst $X = x$, svakoj mogućoj vrednosti ključa

$$Z = z_j, \left(j = 1,\ldots,L^M\right),$$

odgovara jedinstveni šifrat

$$Y = y_j, \left(j = 1,\ldots,L^M\right).$$

Zbog toga, u skladu sa uslovom a), lako se vidi da istom otvorenom tekstu $X = x$ može sa jednakom verovatnoćom odgovarati svaki od L^M mogućih šifrata; zato imamo

$$P(Y = y) = P(Y = y \mid X = x) = L^{-M}.$$

Zbog toga je količina informacije koju nosi šifrat o otvorenom tekstu jednaka nuli, tj. *X* i *Y* su statistički nezavisni, pa stoga suma po modulu *L* ispunjava uslove savršene tajnosti. Kada je $L = 2$, ovaj sistem se svodi na Vernamovu šifru.

5.3.1.1. Sekvencijalni šifarski sistemi

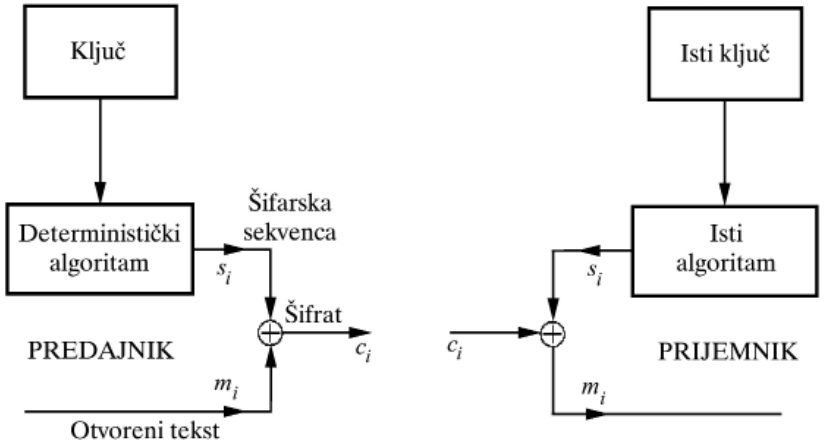
Iako Vernamova šifra garantuje maksimalnu bezbednost, ona nije pogodna za široku praktičnu primenu zato što zahteva jedan simbol tajnog ključa za svaki simbol otvorenog teksta. Imajući u vidu količinu informacija koju u današnje vreme treba šifrovati, pomenuti algoritam se pokazuje nepogodnim za šifrovanje tako velike količine podataka. On se koristi tamo gde je potrebna maksimalna bezbednost, a količina informacija koja se šifruje je minimalna.

U praksi se široko koriste generatori pseudoslučajnih nizova, koji predstavljaju determinističke algoritme za šifrovanje, ali nizovi simbola koje oni generišu imaju osobine slične slučajnim nizovima. Generatori pseudoslučajnih nizova su konačni automati (digitalni automati sa konačnom memorijom) koji koriste kratke ključeve radi započinjanja procesa generisanja. Ovi ključevi moraju biti prisutni na obe strane pre početka komuniciranja. Izlazni niz iz takvog generatora se sabira po modulu 2 sa nizom otvorenog teksta i na taj način se dobija niz šifrata. Na prijemnoj strani se sabira po modulu 2 primljeni niz šifrata sa pseudoslučajnim nizom generisanim pomoću istog ključa, počevši od istog početnog simbola kao i na predajnoj strani. Zbog toga je prijemnik u stanju da rekonstruiše otvoreni tekst.

Evidentno je da nizovi koje generišu konačni automati ne mogu nikada imati potpuno iste osobine kao i slučajni nizovi. Na primer, za razliku od slučajnih nizova, pseudoslučajni nizovi su periodični u širem smislu (što znači da mogu imati aperiodični početak), ali ako su periodi takvih nizova mnogo veći od dužina nizova otvorenog teksta koji će se šifrovati na ovaj način, sistem će se ponašati na sličan način kao i Vernamova šifra.

Osnovna ideja koja stoji iza sekvencijalnih šifara je da se generiše duga i nepredvidljiva sekvenca simbola iz nekog alfabeta (npr. binarnog) na osnovu kratkog ključa izabranog na slučajan način. Sekvencijalna šifra sa generatorom pseudoslučajnog niza je aproksimacija Vernamove šifre, utoliko bolja ukoliko je pseudoslučajni niz bliži po karakteristikama autentičnom slučajnom nizu.

Principska šema sekvencijalnog šifarskog sistema prikazana je na sl. 5.3.1. Ako se koristi binarni alfabet, predajnik *A*, sa kratkim (tajnim) ključem i determinističkim (javnim) algoritmom generiše binarni niz $\{s_i\}$ čiji elementi se sabiraju po modulu 2 sa odgovarajućim bitima otvorenog teksta $\{m_i\}$, i na taj način se dobijaju biti šifrata $\{c_i\}$. Niz $\{c_i\}$ se šalje kroz javni komunikacioni kanal.



Sl. 5.3.1 – Principska šema sekvencijalnog šifarskog sistema

Na prijemnoj strani, strani *B*, sa istim ključem i istim determinističkim algoritmom, generiše se isti šifarski niz $\{s_i\}$, koji se sabira po modulu 2 sa šifratom $\{c_i\}$, i na taj način se rekonstruišu biti otvorenog teksta $\{m_i\}$. Treba uočiti takođe da je sekvencijalni šifarski sistem u ovom slučaju involutivan, zato što su procesi šifrovanja i dešifrovanja identični.

Nije lako utvrditi kada je binarni niz dovoljno bezbedan za upotrebu u kriptografiji, pošto ne postoji opšti i unificirani kriterijum koji bi služio za ocenu takvih nizova. Međutim, može se naznačiti niz zahteva koje svaki šifarski niz mora da zadovolji da bi se mogao koristiti u sekvencijalnom šifarskom sistemu. Najvažniji takvi zahtevi su:

- **Period** – Period šifarskog niza mora da bude bar jednake dužine kao i dužina niza koji se šifruje. U praksi, generišu se nizovi čiji je period mnogo redova veličine veći od dužine niza koji se šifruje.
- **Statističke osobine** – U slučajnom nizu, različiti podstringovi zadate dužine moraju biti uniformno raspodeljeni celom njenom dužinom.

Golomb je formulisao tri postulata koje jedan konačni binarni niz mora da zadovolji da bi bio nazvan pseudoslučajnim [7]. Da bi se formulisali ovi principi, potrebno je prethodno definisati neke pojmove.

Ako je dat binarni niz, serijom dužine *k* se naziva niz sukcesivnih *k* jednakih bita između različitih bita. Na primer, u binarnom nizu

...0100110100**111**0110010**000**1101010**000**1...

nalaze se, između ostalog, 2 serije nula (gaps) dužine 3 i jedna serija jedinica (block) iste dužine.

Funkcija autokorelacije $AC(k)$ jednog periodičnog niza perioda T se definiše kao

$$AC(k) = (A-D)/T$$

gde A i D predstavljaju respektivno broj koincidencija i nekoincidencija između razmatranog niza i njega samog ciklično pomerenog za k pozicija. Ako je k multipl od T, autokorelacija je u fazi i $AC(k)=1$. Ako T ne deli k, autokorelacija je van faze i $AC(k)$ uzima vrednosti na segmentu [-1, 1].

Sada se Golombovi postulati pseudo-slučajnosti mogu formulisati na sledeći na-čin:

G1: U svakom periodu razmatranog niza, broj jedinica mora biti približno jednak broju nula. Konkretnije, razlika između broja jedinica i nula ne sme preći 1.

G2: U svakom periodu razmatranog niza polovina serija od ukupnog broja uo-čenih serija ima dužinu 1, četvrtina ima dužinu 2, osmina dužinu 3 itd.. Istovremeno za svaku pomenutu seriju važi da je jednak broj serija jedinica i nula.

G3: Autokorelaciona funkcija $AC(k)$ van faze je konstantna za svaku vrednost k.

Konačna sekvenca koja zadovoljava ova tri postulata naziva se PN sekvenca (Pseudo-Noise). Ona poseduje sve karakteristike uniformno distribuirane binarne sekvence.

Nepredvidljivost – Ako je dat deo šifarskog niza proizvoljne dužine, kripto-analitičar ne može da predvidi sledeći bit te sekvence sa verovatnoćom većom od 1/2. Jedna od mera nepredvidljivosti sekvence je njena linearna složenost, a jedan od algoritama za njeno izračunavanje je algoritam Berlekamp-Massey.

Lakoća implementacije – Sekvenca mora da bude takva da ju je lako generisati elektronskim sredstvima, radi praktične primene u procesu šifrovanja/dešifrovanja. To uključuje niz tehničkih aspekata: brzina generisanja (npr. reda Mbit/s ili više radi primene u širokopojasnim komunikacijama), troškovi, veličina sklopa za generisanje, broj elektronskih komponenata potrebnih za generisanje, potrošnja, itd., koji se moraju imati u vidu prilikom implementacije generatora šifarske sekvence.

Generatori pseudoslučajnih nizova mogu biti zasnovani na linearnim kongruencijama, pomeračkim registrima sa linearnom ili nelinearnom povratnom spregom, itd. Takođe, pomenute elementarne strukture mogu služiti kao osnovni elementi za konstruisanje složenijih šema.

Generatori koji se zasnivaju na linearnim kongruencijama koriste rekurentne relacije tipa

$$X_{i+1}=aX_i+b(\mathrm{mod}m)$$

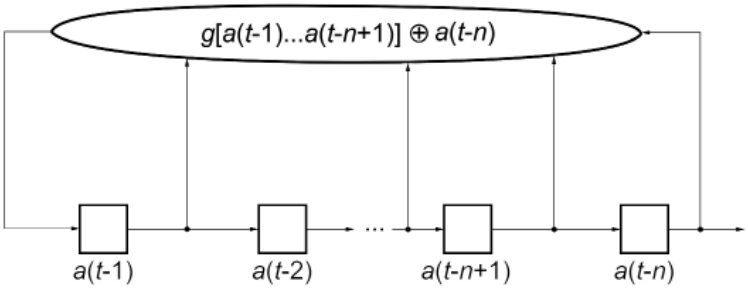
gde su (a, b, m) parametri koji karakterišu generator i mogu da se koriste kao tajni ključ. X_0 je seme koje inicijalizuje proces generisanja. Ako su parametri izabrani na pogodan način, brojevi X_i neće se ponoviti dok potpuno ne pokriju segment [0, *m*-1]. Na primer, niz generisan rekurentnom relacijom

$$X_{i+1}=5X_i+3(\mathrm{mod}16)\ gde\ je\ X_0=1\ je$$

$$\{1,8,11,10,5,12,15,14,9,0,3,2,13,4,7,6,1,8,...\}$$

Nizovi generisani linearnim kongruencijama nisu kriptografski bezbedni. Ako je dat dovoljno dug deo izlaznog niza iz generatora ovog tipa, mogu se rekonstruisati parametri *m*, *a*, *b*.

Pomerački registar sa povratnom spre-gom sastoji se od n flip-flopova (stepena) i jedne funkcije povratne sprege *g* takve da se svaki novi element izlaznog niza *a(t)* za *t>n* može izraziti preko *n* prethodnih elemenata *a(t-n), a(t-n+1),...,a(t-1)*, Sl 5.3.2.. Sadržaj flip-flopova se pomera za jedno mesto u smeru strelica pri svakom takt impulsu, tako da se svaki novi element niza *a(t)* postavlja na prvu poziciju sleva, Sl. 5.3.2. Sadržaj pomeračkog registra između dva takt impulsa naziva se stanje registra; početno stanje registra odgovara njegovom sadržaju na početku procesa generisanja.



Sl. 5.3.2 – Pomerački registar sa povratnom spregom

Dijagram stanja pomeračkog registra (a samim tim i njegovog izlaznog niza) je cikličan ukoliko funkcija *g* povratne sprege nije singularna, tj. ukoliko je njen oblik

$$a(t)=g[a(t-1),a(t-2),...,a(t-n+1)] \oplus a(t-n)$$

($\oplus$ označava operaciju isključivo ili (Exclusive OR - XOR)). U protivnom, novi element *a(t)* ne bi imao konstantu *a(t-n)*, koja bi se izgubila pri sledećem pomeraju.

Period izlaznog niza zavisi od broja stepena registra i karakteristika funkcije *g*. Maksimalni period koji može dostići niz ovog tipa odgovara maksimalnom broju različitih stanja registra. Ako registar ima *n* memorijskih jedinica, maksimalni period je 2^n. Ključ kod ovog tipa generatora sastoji se od početnog stanja registra i funkcije povratne sprege.

Ako je funkcija povratne sprege *g* nelinearna, period izlaznog niza može biti 2^n. Međutim, problem sa ovakvim generatorom je u tome što nema sistematskog metoda za njegovu analizu. Nizovi koje generišu takvi registri mogu da imaju male cikluse koji se beskonačno ponavljaju, što sa kriptografske tačke gledišta nije povoljno. Ciklus koji će se pojaviti zavisi od početnog stanja. Ako je dužina ciklusa manja od 2^n, statističke osobine izlaznog niza neće zadovoljavati prvi i drugi Golombov postulat. Čak i ako period ima maksimalnu dužinu 2^n . U tom slučaju izlazni niz se naziva De Bruijnov niz reda *n* [8]. Autokorelaciona funkcija takvog niza ne zadovoljava treći Golombov postulat.

Najpogodnijim elementarnim strukturama za generisanje pseudoslučajnih nizova smatraju se pomerački registri sa linearnom povratnom spregom. Funkcija povratne sprege kod takvih registara ima sledeći oblik

$$a(t)=c_1a(t-1) \oplus c_2a(t-2) \oplus ... \oplus c_na(t-n)$$

gde je $c_i \in \{0,1\}$ i $c_n=1$.

Očigledno, početno stanje ne može se sastojati od samih nula, pošto bi u tom slučaju izlazni niz bio identički jednak nuli. Maksimalan broj različitih stanja takvog registra jednak je 2^n-1.

Pomeračkom registru sa linearnom po-vratnom spregom može se pridružiti polinom povratne sprege stepena *n*

$$f(x)=1+c_1x+c_2x^2+...+c_nx^n$$

sa nezavisno promenljivom *x* i koeficijentima iz skupa {0,1}. U zavisnosti od karakteristika ovog polinoma, period izlaznog niza može zavisiti od početnog stanja (ako je polinom svodljiv), može biti nezavisan od početnog stanja ali da njegova dužina deli 2^n-1 (ako je polinom nesvodljiv), ili može biti nezavisan od početnog stanja, a da njegova dužina bude 2^n-1 (ako je polinom primitivan). Primitivni polinomi su najpogodniji za kriptografske primene, pošto u tom slučaju izlazni niz iz takvog pomeračkog registra zadovoljava sve Golombove postulate.

Broj primitivnih polinoma stepena *n* dat je sledećim izrazom

$$\phi\left(2^n-1\right)/n$$

gde je $\phi(x)$ Eulerova funkcija koja označava broj pozitivnih celih brojeva manjih od *x* i uzajamno prostih sa *x*. Sekvenca koju generiše pomerački registar sa linearnom povratnom spregom sa primitivnim polinomom povratne sprege naziva se sekvenca maksimalne dužine ili m-sekvenca.

Na žalost, zbog linearnosti, izlazni niz iz pomeračkog registra sa linearnom povratnom spregom je lako predvidljiv. Ako poznajemo 2*n* uzastopnih bita izlaznog niza iz takvog registra, postavljanjem i rešavanjem sistema linearnih jednačina sa *n* nepoznatih možemo odrediti:

- Početno stanje registra (*n* prvih bita).
- Koeficijente c_i, (i=1,...n).

Svaka binarna sekvenca može biti generisana pomoću pomeračkog registra sa linearnom povratnom spregom (LFSR - Linear Feedback Shift Register). Dužina minimalnog LFSR koji može da generiše zadatu binarnu sekvencu naziva se linearna složenost *LC*. U praksi, za određivanje linearne složenosti koristi se algoritam Berlekamp-Massey, kvadratne kompleksnosti [9]. Očigledno, linearna složenost m-sekvence je *n*.

Da bi se povećala linearna složenost pseudoslučajnog niza, izlazni nizovi više pomeračkih registara sa linearnom povratnom spregom mogu se kombinovati pomoću nelinearne funkcije, ili se nekoliko pozicija jednog takvog registra mogu kombinovati pomoću nelinearne funkcije.

5.3.1.2. Blok šifra

Blok šifrom se naziva ona kod koje se originalna poruka šifruje po grupama (blokovima) od dva i više elemenata. Kod blok šifara:

- Način šifrovanja svakog simbola zavisi od načina šifrovanja susednih simbola.
- Svaki blok simbola se šifruje uvek na isti način, nezavisno od mesta koje zauzima u poruci.
- Jednake poruke, šifrovane sa istim klju-čem, uvek daju jednake šifrate.
- Da bi se dešifrovao deo poruke, nije neophodno dešifrovati je od početka, dovoljno je dešifrovati blok koji nas interesuje.

Svaka blok šifra sastoji se od četiri ele-menta:

1. Inicijalna transformacija.
2. Jedna kriptografski slaba funkcija, ponovljena *r* puta ("rundi").
3. Finalna transformacija.
4. Algoritam za ekspanziju ključa.

Inicijalna transformacija može sadržati jednu ili dve funkcije. Prva randomizuje ulazne podatke, radi skrivanja blokova koji sadrže samo jedinice ili samo nule, i obično ne zavisi od ključa. Druga funkcija otežava neke napade na ovakve sisteme, kao npr. linearnu ili diferencijalnu kriptoanalizu. Ova funkcija zavisi od ključa.

Svaka runda se sastoji od jedne nelinearne funkcije, na koju utiču i delovi ključa i delovi ulaznih podataka, koja može biti jednosmerna ili ne. Nelinearna funkcija može sadržati samo jednu veoma kompleksnu operaciju ili niz sukcesivnih različitih jednostavnijih transformacija. Runde se međusobno povezuju sabiranjem po modulu 2, bit za bit, sa podacima koji dolaze iz prethodne runde ili iz inicijalne transformacije. Na taj način se formira involutivna transformacija, kada se ponovi identičan proces (ali uz ključ dešifrovanja dat obrnutim redom), čime se rekonstruiše otvoreni tekst.

Finalna transformacija služi da bi operacije šifrovanja i dešifrovanja bile simetrične.

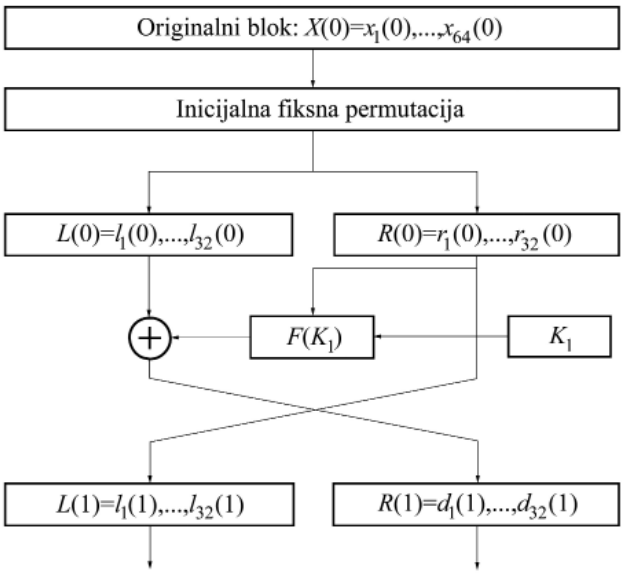
Algoritam za ekspanziju ključa ima za cilj pretvaranje ključa obično ograničene dužine u skup podključeva koji se mogu sastojati od većeg broja bita.

Primeri blok šifara su sledeći: LUCIFER, DES, FEAL, IDEA, RC5, SKIPJACK, BLOWFISH, TWOFISH, AES (RIJNDAEL), itd.

DES

Blok šifra najviše korišćena u praksi je DES (Data Encryption Standard), koji je NBS (National Bureau of Standards) uveo u SAD 1974. Dužina bloka kod ove šifre je 64 bita, a dužina ključa je 56 bita. DES alternativno šifruje dve polovine bloka. Najpre se vrši inicijalna fiksna permutacija bita u bloku. Zatim se blok deli na dve polovine. Posle toga se realizuje jedna modularna operacija koja se ponavlja 16 puta ("rundi"). Ova operacija

se sastoji od sume po modulu 2 leve polovine bloka sa funkcijom $F(K_i)$ desne strane bloka, na koju utiče i podključ K_i, i=1,...,16, gde je *i* redni broj runde. Zatim leva i desna polovina bloka menjaju mesta. Na sl. 5.3.3 je prikazana inicijalna transformacija i prva runda DES-a.



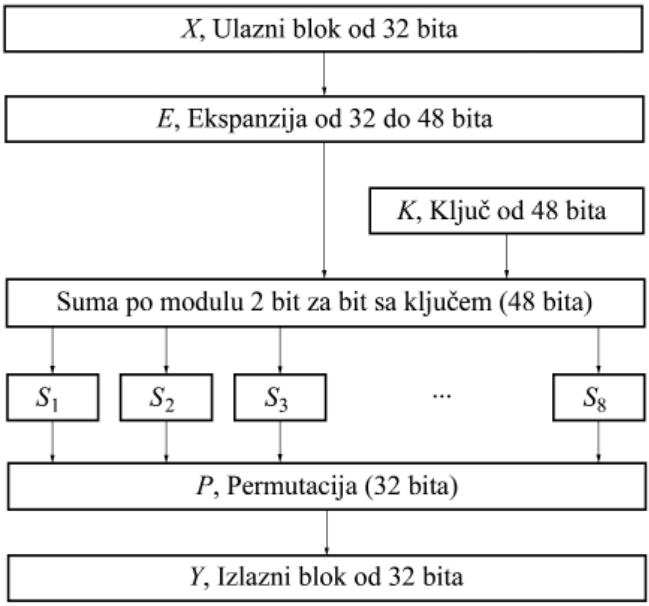
Sl. 5.3.3 – Inicijalna transformacija i prva runda DES-a

U 16. rundi se izostavlja razmena mesta leve i desne polovine bloka, a algoritam se završava finalnom fiksnom permutacijom bita u bloku koja je inverzna inicijalnoj.

DES realizuje involutivnu transformaciju i zato nije potrebno invertovati funkciju *F* u algoritmu za dešifrovanje. Zato *F* može da bude tzv. jednosmerna funkcija, koja sadrži nelinearne operacije.

Funkcija *F* je skup operacija koje se kombinuju na način prikazan na Sl. 5.3.4.

Prva manipulacija se sastoji od formiranja vektora od 48 bita, na osnovu početna 32 bita, putem linearne ekspanzije. Zatim se kombinuje lokalni ključ od 48 bita sa prethodno generisanim vektorom sabiranjem po modulu 2, bit za bit, čime se dobija drugi vektor od 48 bita, koji se deli na 8 grupa od po 6 bita. Svaka od ovih grupa ulazi u jednu od 8 funkcija koje se nazivaju "S-box". Ove tablice su odgovorne za nelinearnost DES-a. Iz svake tablice izlaze 4 bita. Kada se promeni samo jedan bit na ulazu, promene se bar 2 bita izlaza. Na kraju, informacija prolazi kroz "P-box", što je jedna fiksna permutacija, izabrana na takav način da difuzija bita bude maksimalna u bloku od 32 bita.



Sl. 5.3.4 – Struktura funkcije F u DES-u

Iako DES koristi ključ od 64 bita, prva operacija koja se realizuje je njegova redukcija na 56 bita, eliminacijom jednog od svakih osam bita. Zatim se vrši preuređenje preostalih bita. Potom se generiše 16 podključeva potrebnih u 16 rundi algoritma. Svaki podključ se sastoji od 48 bita. Za vreme dešifrovanja oni se koriste obrnutim redom u odnosu na onaj korišćen tokom šifrovanja. Podključevi se generišu na sledeći način: najpre se ključ od 56 bita podeli na dve polovine od po 28 bita. Zatim se te polovine rotiraju ulevo jedan ili dva bita, u zavisnosti od runde. Posle rotiranja, polovine se ponovo sastave i tako se ponovo dobije 16 grupa od po 56 bita. Od ovih bita se izabere po 48 bita iz svake grupe, čime se konačno dobija 16 podključeva. Ovaj proces se naziva "permutacija sa kompresijom". Izabrani biti su jednaki za sve podključeve.

Osnovne osobine DES-a su:

- Međusobna zavisnost simbola – Svaki bit šifrata je jedna složena funkcija svih bita ključa i svih bita otvorenog teksta.
- Promena ulaznih bita – Promena jednog bita poruke prouzrokuje promenu približno 50% bita bloka šifrata.
- Promena bita ključa – Promena jednog bita ključa prouzrokuje promenu približno 50% bita bloka šifrata.
- Slabi ključevi – Postoji četiri slaba ključa koji omogućavaju lako dekriptovanje šifrovane poruke, zato što su u slučaju upotrebe tih ključeva svi podključevi

K_1 do K_{16} međusobno jednaki. Posto-ji 28 "delimično slabih" ključeva koji omogućavaju lako dekriptiranje šifrovane poruke, zato što su u slučaju upotrebe tih ključeva samo dva ili četiri podključa međusobno različiti.

- Greška pri prenosu dela šifrata prostire se na ceo blok kome taj deo pripada ("propagacija greške").

Jedan od problema pri upotrebi DES-a sastoji se u tome što je dužina ključa koji ova šifra koristi nedovoljna kada se ima u vidu današnje stanje razvoja tehnologije. Jasno je da ključ dužine 56 bita ne obezbeđuje dovoljan nivo bezbednosti imajući u vidu procesne mogućnosti savremenih računara i nivo integracije čipova [10]. Takođe su objavljeni i specijalni napadi na blok šifre, npr. na DES, kao što su linearna i diferencijalna kriptoanaliza. Više detalja o ovim kriptoanalitičkim napadima se može naći u [11].

AES (RIJNDAEL)

Zbog slabosti DES-a, u SAD su odlučili da ga zamene novom blok-šifrom, nazvanom AES (Advanced Encryption Standard) [12], [13]. Konačna verzija algoritma AES bila je izabrana između 6 kandidata. Kandidat pod imenom Rijndael je bio izabran, pa je tako postao AES.

Rijndael je iterativna blok-šifra sa promenljivom dužinom bloka, kao i sa promenljivom dužinom ključa. Ove dužine mogu biti 128, 192 i 256 bita. Osnovni element ove šifra se naziva Stanje (State). State je matrica sa 4 vrste i *Nb* kolona, gde je *Nb* jednako dužini bloka podeljenoj sa 32. Ključ je takođe dat matricom sa 4 vrste i *Nk* kolona, gde je *Nk* jednako dužini ključa podeljenoj sa 32. Broj rundi *Nr* kod ove šifre je takođe promenljiv i zavisi od vrednosti *Nb* i *Nk*. *Nr* uzima vrednosti između 10 i 14.

Transformacija u okviru jedne runde sastoji se od 4 koraka:

- Nelinearna supstitucija bajtova (ByteSub).
- Ciklični pomeraj vrsta matrice State (ShiftRow).
- Množenje kolona matrice State fiksnim polinomom po modulu X^4+1 (MixColumn).
- Sabiranje ključa runde sa matricom State (RoundKey).

Da bi algoritam dešifrovanja bio što sličniji algoritmu šifrovanja, poslednja runda ne sadrži korak MixColumn.

Transformacija ByteSub je nelinearna transformacija bajtova, koja nezavisno transformiše svaki bajt matrice State. Tablica supstitucije (pod imenom S-box) je invertibilna i sastoji se od dve transformacije: multiplikativna inverzija u GF (2^8) bajta, u kojoj se 00 transformiše u samog sebe, i afina transformacija (nad GF (2)), definisana još jednom matricom.

Inverzna transformacija od ByteSub sadrži inverznu tablicu od ByteSub. Dobija se inverzijom matrice afine transformacije iz ByteSub i računanjem multiplikativne inverzije rezultata u GF (2^8).

Transformacija ShiftRow ciklički pomera vrste matrice State na različite načine: vrsta *i* se pomera za C_i pozicija, gde C_i zavisi od dužine bloka *Nb, i=0,...,3.* Vrednosti C_i se nalaze između 1 i 4.

Inverzna transformacija od ShiftRow pomera vrstu *i* za (Nb-C_i) pozicija, *i=1,...,3* .

U transformaciji MixColumn, kolone matrice State se smatraju polinomima nad GF (2^8) i množe se fiksnim polinomom $3X^3+X^2+X+2$ po modulu X^4+1.

Inverzna transformacija od MixColumn je slična transformaciji MixColumn: svaka kolona matrice State se množi fiksnim polinomom $11X^3+13X^2+9X+14$ po modulu X^4+1.

U transformaciji RoundKey, ključ runde se sabira sa State po modulu 2, bit za bit. Dužina ključa runde je jednaka *Nb*. Ovaj ključ se dobija od šifarskog ključa (Cipher key) pomoću posebnog algoritma (Key Shedule Algorithm).

Transformacija RoundKey je autoinvertibilna.

Algoritam Key Shedule sastoji se od dve komponente: ekspanzija ključa i izbor ključa runde. Ekspanzija ključa transformiše šifarski ključ (Cipher Key) u ključ veće dužine, čijih prvih *Nk* nizova od po 4 bajta su jednaki onima iz Cipher Key. Postoji razlika između algoritama ekspanzije u zavisnosti od toga da li je $Nk \leq 6$ ili $Nk > 6$. Algoritam za izbor ključa runde koristi 6 nizova od po 4 bajta za svaku rundu, prvih 6 za prvu rundu, drugih 6 za drugu itd.

Slabi, kao i delimično slabi ključevi pra-ktično ne mogu da se pojave kod Rijndael-a, pošto algoritmi šifrovanja i dešifrovanja koriste različite komponente. Ova šifra je takođe otporna na linearnu i diferencijalnu kriptoanalizu, kao i na neke druge publikovane napade na blok-šifre.

NAČINI RADA

Blok-šifre operišu nad redukovanim skupovima podataka. One su pogodne za šifrovanje kratkih poruka, kao što su ključevi, identifikacioni podaci, potpisi, lozinke itd., ali nisu pogodne za šifrovanje velikih količina podataka, kao što su formatirani tekst, listinzi programa, tabele i naročito grafičke datoteke, pošto se struktura takvih dokumenata lako određuje.

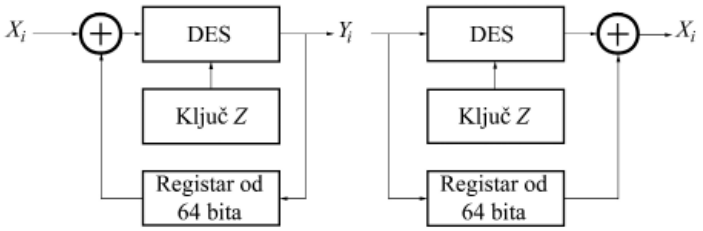
Direktna upotreba blok-šifre se naziva "Elektronska kodna knjiga" (Electronic Codebook, ECB). Takođe, svaka blok-šifra se može upotrebiti u još tri načina rada:

- Ulančavanje šifrovanih blokova (Cipher Block Chaining, CBC).
- Šifrat u povratnoj sprezi (Cipher Feedback, CFB).
- Izlazni niz u povratnoj sprezi (Output Feedback, OFB).

Pretpostavlja se da je dužina bloka *n*. U svim primerima koji se u nastavku opisuju koristi se DES, kao šifra najčešće upotrebljavana u praksi.

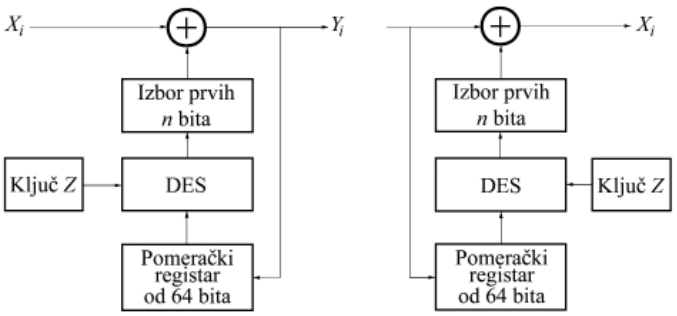
Principska šema načina rada blok-šifre u kome se ulančavaju šifrovani blokovi prikazana je na Sl. 5.3.5. Na početku se u pomerački registar uvodi *n* bita inicijalnog vektora

(VI), koji ne mora da se drži u tajnosti, ali je pogodno da se generiše na slučajan način. U ovom modu blok-šifra se pretvara u sekvencijalnu šifru, jednake poruke se mogu šifrovati na različite načine promenom VI, propagacija grešaka u prenosu se ograničava, a prostor koji razapinje ključ se ne menja.



Sl. 5.3.5 – Način rada blok-šifre u kome se ulančavaju blokovi šifrata

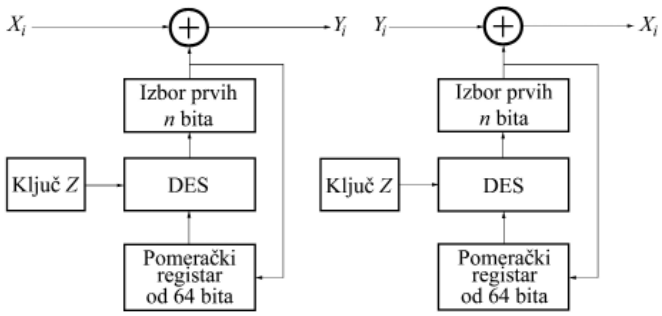
Principska šema načina rada blok-šifre kod koga je šifrat u povratnoj sprezi prikazana je na Sl. 5.3.6. Na početku se u pomerački registar uvodi n bita inicijalnog vektora (VI) koji ne mora da se drži u tajnosti, ali je pogodno da se generiše na slučajan način. Otvoreni tekst se deli na blokove od po m bita. Blokovi se sabiraju po modulu 2, bit za bit, gde m može da varira između 1 i n. Pomerački registar dužine n bita se pomera ulevo m bita posle šifrovanja svakog bloka. U ovom načinu rada blok-šifra se pretvara u sekvencijalnu šifru, jednake poruke se mogu šifrovati na različite načine promenom vektora VI, ograničava se propagacija grešaka u prenosu, prostor koji razapinje ključ ne menja se, a šifra je samosinhronišuća.



Sl. 5.3.6 – Način rada blok-šifre sa šifratom u povratnoj sprezi

Principska šema načina rada blok-šifre sa izlaznim nizom u povratnoj sprezi prikazana je na Sl. 12.3.7. Na početku se u pomerački registar dužine n bita uvodi inicijalni vektor (VI) koji mora da se drži u tajnosti i da bude slučajan. Otvoreni tekst se deli na blokove od po m bita. Blokovi od po m bita se sabiraju po modulu 2, bit za bit, pri čemu dužina bloka može da varira između 1 i n. Pomerački registar dužine n bita se pomera

ulevo *m* bita posle šifrovanja svakog bloka. U ovom načinu rada blok-šifra se pretvara u sekvencijalnu šifru, koja se koristi kao generator šifarske sekvence, jednake poruke se mogu šifrovati na različite načine promenom vektora VI, nema propagacije grešaka, prostor koji razapinje ključ se udvostručava i šifra nije samosinhronišuća.



Sl. 5.3.7 – Način rada blok-šifre sa izlaznim nizom u povratnoj sprezi.

Jedini način na koji se može povećati prostor koji razapinje ključ blok-šifre je multiplikacija šifre, odnosno ponavljanje šifre *n* puta, koristeći *n* međusobno nezavisnih ključeva.

Očigledno je da se na ovakav način bezbednost povećava, ali ne uvek proporcionalno dužini ključa. Na primer, za DES, efektivna dužina ključa iznosi približno

$$l = 56 \cdot \left\lfloor \frac{n}{2} \right\rfloor bita$$

umesto $56 \cdot n$. Ako bi *n* bilo jednako 3, dužina ključa bi bila 112 bita.

Treba imati u vidu takođe da tako spregnuta šifra ne sme da formira algebarsku grupu. U tom slučaju bi dve sukcesivne šifre sa dva različita ključa bile ekvivalentne jednoj jedinoj šifri. Može se pokazati da ni DES ni Rijndael ne čine algebarsku grupu.

5.3.2 Asimetrični šifarski sistemi

Šifarski sistem sa tajnim ključem je familija parova funkcija (E_k, D_k) za svaki ključ *k* iz skupa ključeva K, definisana na sledeći način: $E_k: M \times C$ i $D_k: C \times M$, gde su M i C skupovi otvorenih tekstova i šifrata, respektivno, takva da za svaki otvoreni tekst *m* iz M važi $D_k(E_k(m))=m$.

Da bi se koristio ovakav sistem, korisnici *A* i *B* se dogovore da uzmu tajni ključ *k* iz K. Ako *A* želi da pošalje poruku *m* iz M korisniku *B*, šifruje je pomoću funkcije E_k, $E_k(m)=c$, i šalje rezultat *c* korisniku *B*. Da bi rekonstruisao originalnu poruku, B dešifruje primljeni šifrat *c* pomoću funkcije D_k, $D_k(c)=D_k(E_k(m))=m$.

U kriptografiji se smatra "lakim" proračun koji se može izvršiti u kratkom vremenu. Za probleme koji se ne mogu rešiti u prihvatljivom vremenskom periodu, koristeći najbolji poznati algoritam i najbolju raspoloživu tehnologiju koristi se termin "teški" ili "intraktabilni". Parovi funkcija (E_k,D_k) moraju biti "laki" za izračunavanje za korisnike i morali bi biti "teški" za izračunavanje za kriptoanalitičara koji poznaje samo *c*, tako da ne može da rekonstruiše ni *m* ni *k*.

Problemi koji se sreću u kriptografiji sa tajnim ključevima su sledeći:

1. Distribucija ključeva – Dva korisnika moraju da izaberu tajni ključ pre početka komunikacije i da za njegovo prenošenje koriste siguran kanal. Ovakav siguran kanal nije uvek na raspolaganju.
2. Manipulacija ključevima – U mreži sa *n* korisnika, svaki par korisnika mora da ima svoj sopstveni tajni ključ, što čini ukupno $m(n-1)/2$ ključeva za tu mrežu.
3. Nemogućnost realizacije digitalnog potpisa – U šifarskim sistemima sa tajnim ključevima nema mogućnosti, u opštem slučaju, za digitalno potpisivanje poruka, tako da onaj koji prima poruku ne može da bude siguran da je onaj koji mu je poslao poruku zaista njen autor.

5.3.2.1. Pojam sistema sa javnim ključem

Radi uvođenja šifarskih sistema sa javnim ključevima, definiše se jednosmerna funkcija (One-Way Function, OWF) $f:M\text{x}C$ kao invertibilna funkcija, takva da je "lako" izračunati $f(m)=c$, dok je "teško" izračunati $f^{-1}(m)=c$. Za jednosmernu funkciju se kaže da poseduje zamku (Trapdoor One-Way Function, TOF) ako se može lako invertovati pod uslovom da se poznaje dodatna informacija. Takva dodatna informacija se naziva zamka.

Šifarski sistem sa javnim ključem se definiše kao familija jednosmernih funkcija sa zamkom,$\{f_k\}$, za svaki ključ *k* iz K, takva da se zamka $t(k)$ može lako odrediti. Pored toga, za svako *k* iz K potrebno je definisati efikasan algoritam za izračunavanje f_k, ali takav da je određivanje *k* i $t(k)$ intraktabilno.

Radi implementacije šifarskog sistema sa javnim ključem, ako je data familija jednosmernih funkcija sa zamkom, svaki korisnik *U* izabere na slučajan način ključ *u* iz K i publikuje E_u pomoću koga može da se izračuna f_u. E_u je njegov javni ključ, dok je zamka $t(u)$, neophodna za invertovanje f_u, njegov tajni ključ.

Ako korisnik *A* želi da pošalje poruku *m* drugom korisniku *B*, pronađe u registru javnih ključeva javni ključ korisnika *B*, E_b, i pošalje $f_b(m)=c$ korisniku *B*. Kako jedino *B* može da invertuje f_b, jedino on može da rekonstruiše poruku *m*: $f_b^{-1}(c) = f_b^{-1}(f_b(m))=m$.

Problem sa sistemima sa javnim ključevima sastoji se u tome što nije dokazana egzistencija ni jednosmernih funkcija ni jednosmernih funkcija sa zamkom. Uprkos tome, postoje dve funkcije koje se smatraju kandidatima za funkcije sa pomenutim svojstvima. Prva od njih je proizvod celih brojeva, čija inverzna funkcija je faktorizacija dobijenog

broja, a druga je diskretna eksponencijacija, čija inverzna funkcija je diskretni logaritam. Ove dve funkcije su lake za izračunavanje, dok se veruje da to nije slučaj sa njihovim inverznim funkcijama. Na primer, ako je dat broj n, veruje se da je teško odrediti njegovu dekompoziciju na proste faktore i, sa druge strane, ako su dati brojevi a i b, veruje se da je teško izračunati x takav da je $a^x=b$. Na taj način, sigurnost sistema sa javnim ključevima koji se danas koriste u praksi zavisi od broja operacija potrebnog da bi se invertovale pomenute funkcije i još uvek nije dokazano da ne postoji algoritam za njihovo lako invertovanje.

Pojam sistema sa javnim ključevima uveli su Diffie i Hellman 1976. godine. Prvi takav sistem koji su oni definisali bio je protokol, poznat pod imenom razmena ključeva Diffie-Hellman. Radi se o sledećem:

1. Dva korisnika, A i B, izaberu javno konačnu multiplikativnu grupu, G, reda n i jedan njen element $\alpha \in G$.
2. A generiše slučajan broj a, izračuna α^a u G i pošalje ovaj element korisniku B.
3. B generiše slučajan broj b, izračuna α^b u G i pošalje ovaj element korisniku A.
4. A primi α^b i izračuna $(\alpha^b)^a$ u G.
5. B primi α^a i izračuna $(\alpha^a)^b$ u G.

Na taj način, A i B poseduju zajednički tajni element iz grupe G: $\alpha^{a}b$. Kriptoanalitičar S može da poznaje G, n, α^a i α^b i treba da izračuna element α^{ab}. Ali problem je u tome što je taj proračun ekvivalentan izračunavanju diskretnog logaritma. Zato se veruje da je "težak".

Primer: Neka je p prost broj 53. Pretpostavimo da je $G=Z^*_{53}$ i neka je $\alpha=2$ jedan od njenih generatora. Protokol Diffie-Hellman je sledeći niz operacija:

1. A bira $a=29$, izračunava $\alpha^a = 2^{49} \equiv 45 (mod 53)$ i šalje 45 korisniku B.
2. B bira $b=19$, izračunava $\alpha^a = 2^{49} \equiv 45 (mod 53)$ i šalje 12 korisniku A.
3. A prima 12 i izračunava $12^{29} \equiv 21 (mod 53)$.
4. B prima 45 i izračunava $45^{29} \equiv 21 (mod 53)$.

Privatni ključ ili tajna informacija koju sada dele A i B je 21. Kriptoanalitičar S poznaje Z^*_{53}, 2, 45 i 12, ali ne može da rekonstruiše da je informacija koju dele A i B jednaka 21 zato što mora da izračuna diskretni logaritam da bi to odredio.

5.3.2.2. Sistem Rivest-Shamir-Adleman (RSA)

1983. godine Rivest, Shamir i Adleman su patentirali šifarski sistem sa javnim ključevima poznat pod imenom RSA (inicijali autora) [14]. Protokol koji su razvili pomenuti autori je sledeći:

1. Svaki korisnik *U* izabere dva prosta broja (danas se preporučuje da ti brojevi imaju više od 200 cifara) *p* i *q* i računa $n=p\cdot q$. To znači da je grupa koju koristi korisnik *U* Z^*_{53}. Red te grupe je $\varphi(n)= \varphi(p\cdot q)=(p-1)(q-1)$. Korisniku *U* je lako da izračuna ovaj red, pošto zna *p* i *q*.
2. Zatim *U* izabere pozitivan broj *e*, $1 \le e < \varphi(n)$, takav da je uzajamno prost sa redom grupe, tj. takav da je NZD $(e,\varphi(n))=1$.
3. Pomoću generalizovanog Euklidovog algoritma korisnik *U* izračuna inverzni element od *e* u $Z_{\varphi(n)}$, *d*. Znači $e\cdot d\equiv 1(mod\ \varphi(n))$, pri čemu je $1 \le d < \varphi(n)$.
4. Javni ključ korisnika *U* je par (n,e), dok je njegov privatni ključ broj *d*. Naravno, brojevi *p*, *q* i $\varphi(n)$ takođe moraju da se drže u tajnosti.

Ako korisnik A želi da pošalje poruku *m* iz Z_n drugom korisniku B, koristi javni ključ korisnika B, (n_b,e_b), da bi izračunao vrednost $m^{e_b}(mod\ n_b)=c$, koju šalje korisniku B.

Da bi rekonstruisao poruku, B računa $c^{d_b}=(m^{e_b})^{d_b}=m^{e_b d_b}\equiv m(mod n_b)$.

Primer: Razmotrimo kodiranje alfabeta koje transformiše slova A do Z u brojeve 0 do 25 (koristićemo engleski alfabet). Želimo da pošaljemo poruku korisniku B.

Korisnik B bira dva prosta broja: $p_b=281$ i $q_b=167$, računa $n_b=281\cdot 167=46927$ što znači da radi sa grupom Z^*_{46927}.

Red ove grupe je: $\varphi(46927)=280\cdot 166=46480$. *B* bira broj $e_b=39423$ i verifikuje da je $NZS(39423,46480)=1$. Zatim određuje inverzni element od 39423 po modulu 46480. Ovaj broj je $d_b=26767$. Znači javni ključ korisnika *B* je: $(n_b,e_b)=(46927,39423)$, dok ostale vrednosti drži u tajnosti.

Da bismo poslali poruku korisniku *B*, moramo da odredimo na prvom mestu njenu dužinu. Imaćemo u vidu da se kodovanje slova alfabeta vrši u bazi 26. Kako poruka mora da bude element grupe sa kojom radimo, njena dužina ne može da pređe vrednost $n=46927$. Zato ako se ima u vidu da je $26^3=17576<n<456976=26^4$, poruka može da ima najviše tri slova. Ako želimo da pošaljemo dužu poruku, moramo da je podelimo na grupe od po tri slova. U praksi je dužina poruke mnogo veća, pošto je *n* broj sa mnogo više cifara. Ako, na primer, želimo da pošaljemo korisniku *B* poruku *m*="YES", procedura je sledeća:

Pretpostavimo da smo korisnik *A* čiji je javni ključ $(n_a,e_a)=(155011,2347)$ i čiji je privatni ključ $d_a=151267$, pri čemu je $p_a=409$, $q_a=379$ i $\varphi(n_a)=154224$. Da bismo poslali

poruku *m*, moramo da je kodujemo, tj. da je izrazimo u bazi 26 tako da bude element grupe koja se koristi, što znači da pripada Z^*_{46927}:

$$YES=Y\cdot 26^2+E\cdot 26+S=26\cdot 26^2+4\cdot 26+18=$$
$$=16346=m$$

Sada šifrujemo *m* javnim ključem korisnika *B*:

$$c=m^{eb}(modn_b)\ 16346^{39423}(mod46927)=21166.$$

Dekodujemo šifrovanu poruku:

$$c=21166=1\cdot 26^3+5\cdot 26^2+8\cdot 26+2=BFIC$$

Znači, korisniku *B* se šalje sledeći tekst: "BFIC".

Da bi *B* mogao da rekonstruiše poruku, mora da koduje primljene podatke u bazi 26, a zatim da realizuje sledeće operacije:

$$BFIC=21166=1\cdot 26^3+5\cdot 26^2+8\cdot 26+2=c$$

Sada može da rekonstruiše *m* računajući

$$m=c^{db}(modn_b)\ 21166^{2676}(mod46927)=16346.$$

m se dekoduje i dobija se originalni tekst

$$m=16346=24\cdot 26^2+4\cdot 26+18=YES$$

U praksi, radi smanjenja složenosti operacija u šifarskom sistemu RSA, obično se bira mali javni ključ, tako da se poruka može poslati na najbrži mogući način. Mnogi korisnici koriste unutar svojih javnih ključeva isti eksponent (najčešće korišćeni eksponenti su 3 i $2^{16}+1$). Ova činjenica ne kompromituje bezbednost šifarskog sistema i omogućava da šifrovanje poruka bude mnogo brže nego dešifrovanje.

Sa algoritamske tačke gledišta, ako je *k* broj bita modula *n*, za izvršenje operacija sa javnim ključem potrebno je $O(k^3)$ koraka, a za generisanje ključeva potrebno je $O(k^4)$ koraka. Zbog toga je u praktičnoj realizaciji softvera šifarski sistem sa tajnim ključem DES najmanje 100 puta brži od RSA, a u praktičnoj realizaciji hardvera DES je između 1000 i 10000 puta brži od RSA. Ipak, šifarski sistem RSA se koristi u praksi zato što se poruke šifrovane pomoću njega mogu digitalno potpisati.

Bezbednost šifarskog sistema RSA zasniva se na problemu faktorizacije.

5.3.2.3. Drugi algoritmi sa javnim ključevima

Sistem ElGamal

ElGamal je predložio sistem sa javnim ključevima zasnovan na diskretnoj eksponencijaciji nad multiplikativnom grupom konačnog tela Z_p [15]. Ovaj protokol, modifikovan tako da koristi konačnu grupu *G* je sledeći:

- Pretpostavlja se da su poruke elementi grupe *G* i da korisnik *A* želi da pošalje poruku *m* korisniku *B*.
  1. Izabere se konačna grupa *G* i element α iz *G*.
  2. Svaki korisnik *A* izabere slučajni broj *a*, koji će biti njegov tajni ključ, i računa α^a u *G*, koji će biti njegov javni ključ.
- Da bi korisnik *A* poslao poruku *m* drugom korisniku *B*, pod pretpostavkom da su poruke elementi grupe *G*, realizuje sledeće operacije:
  1. *A* generiše slučajan broj ν i računa α^ν u *G*.
  2. *A* pronalazi javni ključ korisnika *B*, α^b, i računa $(\alpha^b)^\nu$ i $m\cdot\alpha^{b\nu}$ u *G*.
  3. *A* šalje par $(\alpha^\nu, m\cdot\alpha^{b\nu})$ korisniku *B*.
- Da bi rekonstruisao originalnu poruku:
  1. *B* računa $(\alpha^\nu)^b$ u *G*.
  2. *B* dobija *m* računajući jedino

$$\frac{m\cdot\alpha^{\nu b}}{\alpha^{\nu b}}$$

Da bi se uprostio gornji protokol, sam ElGamal je preporučio da se operacije izvode unutar multiplikativne grupe tela Z_p. Na taj način, stepeni i proizvodi se računaju po modulu prostog broja *p*.

Bezbednost šifarskog sistema ElGamal zasniva se na problemu diskretnog logaritma.

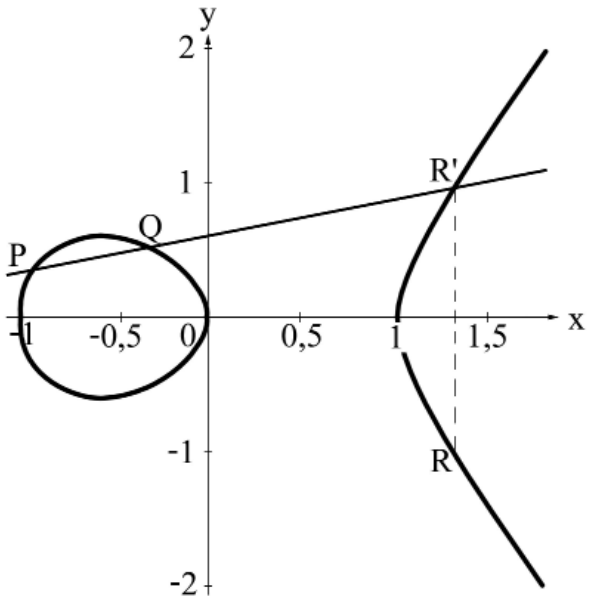
Šifarski sistemi sa eliptičkim krivim

Ako je dato telo *K*, eliptičkom krivom nad *K* se naziva kriva u ravni definisana jednačinom:

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,$$
$$a_i\in K,\ i=1,\ldots,6$$

Eliptička kriva predstavlja specijalan tip algebarske krive sa svojstvom da tačke koje leže na njoj čine aditivnu Abelovu grupu. Neka je *E* eliptička kriva definisana nad konačnim telom GF (*q*), gde je *q* prost broj ili stepen prostog broja p^m. Suma dve tačke u *E* se definiše na sledeći način. Ako su date dve tačke *P,Q*x*E*, prava $\overline{PQ}$ se seče sa *E* u tri tačke (pošto je jednačina koja definiše *E* trećeg stepena): u tački *P*, u tački *Q* i u trećoj tački *R′*. Suma *P*+*Q*=*R* definiše se na način prikazan na Sl. 5.3.7.

Na taj način, množenje koje se izvršava u drugim šifarskim sistemima sa javnim ključem ovde se transformiše u sabiranje dve tačke, dok se eksponencijacija koja se izvršava u drugim sistemima transformiše ovde u proizvod jednog broja iz GF (q) sa jednom tačkom krive. Operacije ovog tipa unutar grupe su lake za implementaciju u hardveru i softveru. Sa druge strane, dokazano je da je problem diskretnog logaritma nad eliptičkom krivom jednako težak za rešavanje kao i nad drugim grupama istog reda. Zbog toga su eliptičke krive korišćene za implementaciju šifarskih sistema zasnovanih na diskretnom logaritmu kao što su Diffie-Hellman [16] i ElGamal sa jednakom bezbednošću, ali sa jednom prednošću koja se sastoji u korišćenju manjih ključeva, za šta je potrebno manje memorije i hardverskih elemenata manjih dimenzija.



Sl. 5.3.7 – Eliptička kriva

5.3.3 Hash funkcije

Šifarski sistemi sa javnim ključevima, kao i sistemi za digitalni potpis mogu biti veoma spori. Takođe, u nekim slučajevima, dužina digitalnog potpisa može biti veća ili jednaka dužini same poruke koja se potpisuje. Da bi se rešili ovi problemi koriste se hash funkcije.

Hash funkcija je izračunljiva funkcija koja primenjena na poruku m promenljive dužine daje njenu reprezentaciju fiksne dužine koja se naziva njenom hash vrednošću $H(m)$. Hash funkcije se definišu na sledeći način:

$$H: M \times M, H(m) = m'$$

U opštem slučaju, *H(m)* je mnogo manjih dimenzija od *m*. Na primer, *m* može da ima dužinu od jednog megabajta, dok *H(m)* može imati svega 64 ili 128 bita.

Sa druge strane, hash funkcije se mogu koristiti za određivanje rezimea nekog dokumenta i njegovo publikovanje, bez objavljivanja njegovog sadržaja.

Jednosmerna hash funkcija je hash funkcija *H* definisana tako da je za svaku komprimovanu poruku m' teško rekonstruisati originalnu poruku *m* za koju važi m'=*H(m)*. Dakle, jednosmerna hash funkcija je hash funkcija koja je takođe i jednosmerna (One Way).

Ako je hash funkcija jednosmerna, tj. teška za invertovanje, takođe se naziva i rezime funkcija (Message-digest function). U tom slučaju, uobičajeno je da se vrednost *H(m)* naziva rezime od *m* ili otisak prsta poruke *m*.

Upotrebom hash funkcija, problem dužine poruke ili digitalnog potpisa se rešava tako što se umesto da se šifruje ili digitalno potpisuje cela poruka *m* potpisuje se ili šifruje samo rezime poruke *H(m)*.

Hash funkcije koje se najviše koriste u kriptografske svrhe su MD2, MD4 i MD5 (Message Digest), koje je predložio Rivest. Ove funkcije daju rezimee dužine 128 bita.

5.3.4 Digitalni potpis

Kriptografija sa javnim ključevima omogućava da bilo koja poruka koju šalje bilo koji korisnik sadrži digitalni potpis, analogan uobičajenom potpisu u papirnoj korespondenciji. Mogućnost digitalnog potpisivanja omogućava korisniku na prijemnoj strani da se uveri da mu je poruku poslao legitiman pošiljalac. Sa druge strane, digitalni potpis daje veću garanciju od običnog potpisa da primljeni dokument nije modifikovan.

Digitalni potpisi se klasifikuju na različite načine:

- Implicitni – ako se nalaze u samoj poruci.
- Explicitni – ako su dodati uz poruku, kao neodvojivi deo.
- Privatni – ako ga može identifikovati jedino neko ko poseduje zajedničku tajnu informaciju sa pošiljaocem.
- Javni (ili istinski) – ako bilo ko može da identifikuje pošiljaoca na osnovu javno dostupne informacije.
- Revokabilni – ako pošiljalac može kasnije da negira da digitalni potpis pripada njemu.
- Irevokabilni – ako primalac može da dokaže da je pošiljalac autor poruke.

Digitalni potpisi moraju se jednostavno kreirati i verifikovati, a teško falsifikovati. Proces digitalnog potpisivanja jedne poruke sastoji se od dva dela: najpre se računa potpis korisnika koji odgovara poruci, koji samo korisnik može generisati na osnovu svog privatnog ključa i poruke koju želi da potpiše, a zatim se šifruje potpis i šalje se javnim kanalom.

Ako *A* želi da digitalno potpiše poruku *m*, šalje šifrovanu poruku *c* korisniku *B* i da bi je digitalno potpisao:

1. *A* računa potpis šifrujući poruku koju treba poslati svojim tajnim ključem:

   $r=f_a^{-1}(m)$, r je potpis korisnika *A* za poruku *m*.

2. *A* određuje digitalni potpis poruke *m* šifrovanjem javnim ključem korisnika *B* potpisa koji je odredio u tački 1:

$s=f_b(r)=f_b(f_a^{-1}(m))$.

B rekonstruiše poruku na isti način kao i bez digitalnog potpisa i da bi verifikovao digitalni potpis korisnika *A*:

1. *B* određuje potpis korisnika *A* za primljenu poruku, calculando

   $f^{-1}{}_b(s)=f^{-1}{}_b(f_b(r))=r$, pomoću svog tajnog ključa.

2. *B* proverava da li je $f_a(r)=f_a(f_a^{-1}(m))=m$.

Da bi poslao digitalni potpis poruke *m* pomoću šifarskog sistema RSA, korisnik *A*, čiji je javni ključ (n_a, e_a) i čiji je tajni ključ d_a, izvršava sledeći niz operacija:

1. Računa svoj potpis šifrujući poruku pomoću svog tajnog ključa: $r=m^{d_a}(\mathrm{mod}n_a)$.
2. Određuje digitalni potpis šifrovanjem pomoću javnog ključa korisnika *B* potpis izračunat u tački 1: $s=r^{e_b}(\mathrm{mod}n_b)$.

Potpisana poruka koju korisnik *A* šalje korisniku *B* je par (c,s), gde je *c* šifrat koji odgovara poruci *m*.

Da bi korisnik *B* mogao da verifikuje da potpis odgovara korisniku *A*, treba da proveri da li važi:

1. $s^{d_b}(\mathrm{mod}n_b) \equiv (r^{e_b}(\mathrm{mod}n_b))^{d_b}(\mathrm{mod}n_b) \equiv$

   $\equiv (r^{e_b d_b}(\mathrm{mod}n_b) = r$

2. $r^{e_a}(\mathrm{mod}n_a) \equiv m^{d_a e_a}(\mathrm{mod}n_a) = m$

Prilikom dodavanja digitalnog potpisa nekoj poruci, mora se imati u vidu da radi određivanja potpisa *r*, poruka *m* mora biti unutar ranga šifrovanja n_a. Na taj način dužina poruke *m* ne samo da mora da bude manja od n_b da bi bila šifrovana, već takođe mora da bude manja i od n_a da bi se mogao generisati potpis pošiljaoca. Sa druge strane, potpis koji se dobije šifrovanjem pomoću tajnog ključa pošiljaoca mora biti unutar ranga šifrovanja n_b, pošto je za određivanje digitalnog potpisa potrebna redukcija po modulu n_b.

Ako se radi o mreži i ako neki korisnik želi da komunicira sa različitim korisnicima unutar te mreže, pogodno je definisati proces kojim se izbegava gornja analiza za svaku poruku koju neko želi da pošalje. Rivest, Shamir i Adleman su predložili protokol orijentisan ka komunikacionoj mreži. Ovaj protokol se sastoji od sledećih koraka:

1. Odredi se prag h (na primer, h $\approx 10^{199}$).
2. Svaki korisnik U publikuje dva para javnih ključeva: (n_u, e_u) i (l_u, f_u). Prvi ključ služi za šifrovanje poruka, a drugi za verifikaciju potpisa.
3. Modul svakog od korisnika mora da ispunjava sledeći uslov: $l_u < h < n_u$.

Sa uslovima gore definisanim, da bi korisnik A poslao korisniku B potpisanu poruku, dovoljno je da blokovi poruke m koja se šalje ispunjavaju sledeći uslov: $0 < \min\{l_u\}$. Kada se poruka podeli na blokove koji ispunjavaju taj uslov, da bi šifrovao poruku m, korisnik A koristi javni ključ korisnika B: (n_b, e_b), i da bi odredio svoj potpis koristi tajni ključ g_a koji odgovara njegovom javnom ključu za digitalno potpisivanje poruka: (l_a, f_a).

Primer: Pretpostavimo da korisnik A određuje potpis za poruku m=*"YES"* i da korisnik B želi da proveri da li je A pošiljalac.

U ovom primeru smatramo da je javni ključ korisnika A $(n_a, e_a)=(34121,15775)$, njegov tajni ključ je $d_a=26623$, pri čemu je $p_a=229$, $q_a=149$ i $\phi(n_a)=33744$.

Sa druge strane, javni ključ korisnika B je $(n_b, e_b)=(46937,39423)$, njegov tajni ključ je $d_b=26767$, pri čemu je $p_b=281$, $q_b=167$ i $\phi(n_b)=46280$.

Kodirana poruka m="YES" je m=16346.

Korisnik A određuje svoj potpis za ovu poruku računajući:

$$r=m^{eb}(\mathrm{mod}n_a) \equiv 16346^{26623}(\mathrm{mod}34121) = 20904$$

zatim određuje digitalni potpis:

$$s=r^{eb}(\mathrm{mod}n_b) \equiv 20904^{39423}(\mathrm{mod}46927)=33261$$

i na kraju dekoduje digitalni potpis:

$$s=33261=1\cdot 26^3+23\cdot 26^2+5\cdot 26+7=BFHX$$

Kompletna poruka koju korisnik A šalje korisniku B sastoji se od šifrata i digitalnog potpisa, tj. od para $(BFIC,BFHX)$.

Kada korisnik B dešifruje poruku koju je poslao korisnik A, proverava digitalni potpis korisnika A, izvršavajući sledeće operacije:

Dekoduje digitalni potpis korisnika A:

$$BHFX = 1\cdot 26^3+23\cdot 26^2+5\cdot 26+7 = 33261=s$$

Određuje potpis korisnika A za datu poruku:

$$r=s^{db}(\mathrm{mod}n_b) \equiv 33261^{36767}(\mathrm{mod}46927) = 20904.$$

Ponovo rekonstruiše poruku:

$$m=r^{ea}(\mathrm{mod}n_a) \equiv 20904^{12775}(\mathrm{mod}34121)=16346.$$

i na kraju dekoduje poruku, poredeći je sa porukom dobijenom direktnim dešifrovanjem:

$$16346=24\cdot 26^2+4\cdot 26+18=YES.$$

Šema koju je konstruisao ElGamal za digitalno potpisivanje poruka je sledeća:

1. *A* generiše slučajan broj *h* takav da je NZD
   $(h,(p-1))=1$.
2. *A* računa element
   $r=\alpha^h \pmod n$.
3. *A* rešava kongruenciju:
   $m=a\cdot r+h\cdot s \pmod{p-1}$.

Digitalni potpis korisnika *A* za poruku *m* je par (r,s).

Da bi primalac poruke proverio potpis korisnika *A*, mora da realizuje sledeće operacije:

1. *B* računa
   $r^s \equiv (\alpha^h)^s \pmod n$ *y* $(\alpha^a)^r \pmod n$.
2. *B* računa
   $(\alpha^a)^r (\alpha^h)^s \pmod n$,
   i proverava da li je to jednako
   $\alpha^m \pmod n$.

Primer: Pretpostavimo da korisnik *A* šalje korisniku *B* svoj digitalni potpis za poruku *m*="HIJO" sa sledećim podacima: grupa koja se razmatra je $Z^*_{15485863}$, generator je α=7, tajni ključevi korisnika *A* i *B* su, respektivno, a=28236 i b=21702 i javni ključevi su 12506884 i 8890431.

A računa svoj digitalni potpis za poruku *m* na sledeći način:

Bira slučajan broj h=90725, uzajamno prost sa redom grupe NZD(90725,15485862)=1.

Računa

$$r = \alpha^h = 7^{90725} \equiv 7635256 \pmod{1548563}$$

Rešava kongruenciju:

$$m\equiv a\cdot r+h\cdot s \pmod{\varphi(n)}$$

tj.

$$128688 \quad 28236\cdot 7635256+90725\cdot s \pmod{15485863}$$

Gornja jednačina se rešava po *s*:

$$s \equiv \frac{128688 - 28236 \cdot 7635256}{90725} \equiv \frac{5211036}{90725} \equiv$$

$$\equiv 5211036 \cdot 11031191 = 11047464 (\text{mod } 15485862)$$

gde se inverzni element od *h* određuje pomoću generalizovanog Euklidovog algoritma. Rešenje je s=11047464.

Potpis korisnika *A* za ovu poruku je dakle:

$$(r,s) = (7635256, 11047464).$$

Da bi proverio potpis korisnika *A*, korisnik *B* računa:

$$(\alpha^h)^s = r^s = 7635256^{11047464} \equiv 8799713 \ (\text{mod } 15485863)$$

Zatim računa:

$$(\alpha^a)^r = 12506884^{7635256} \equiv 1260686 (\text{mod } 15485863)$$

a takođe i vrednost

$$\alpha^m = 7^{128688} \equiv 5362356 (\text{mod} 15485863).$$

Na kraju proverava da li je

$$r^s \cdot (\alpha^a)^r = 8799713 \cdot 1260686 \ \ 5362356$$

$$= 5362356 \equiv \alpha^m (\text{mod } 15485863)$$

Digitalni potpisi generisani u ovom šifarskom sistemu su duži nego u sistemu RSA. Pored toga, ovaj šifarski sistem je sporiji za šifrovanje i proveravanje digitalnog potpisa od RSA.

U praksi se kombinuje hash funkcija i digitalni potpis. Korisnik *A* koji želi da pošalje poruku *m* korisniku *B*, zajedno sa svojim potpisom, šalje $c=f_b(m)$, i kao digitalni potpis šalje potpis dobijen od šifrovanog rezimea $H(m)$. Znači, određuje sledeće:

1. Potpis za rezime poruke: $r=f_a^{-1}(H(m))$.
2. Digitalni potpis za informaciju određenu u tački 1: $s=f_b(r)=f_b(f_a^{-1}(H(m)))$.

Korisnik *B* rekonstruiše poruku na uobičajen način tj. određuje *m* računajući $f_b^{-1}(c)=f_b^{-1}(f_b(m))=m$ i ispituje validnost potpisa korisnika *A*:

1. Računa potpis korisnika *A* za rezime poruke *m*: $r=f_b^{-1}(s)= f_b^{-1}(f_b(r))$.
2. Određuje rezime poruke *m*, $H(m)$: $H(m)=f_a^{-1}(r)= f_a(f_a^{-1}(H(m)))$.
3. Proverava da li primljena poruka koincidira sa vrednošću *H* dobijenom na osnovu već dešifrovane poruke *m*.

5.4 LITERATURA

[1] Computer Security Institute, Inc. "2002 CSI/FBI Computer Crime and Security Survey", Computer Security Issues & Trends, 2002.

[2] S. Garfankel, G.Spafford, "Web Security and Commerce", Cambridge, MA: O'Reilly and Associates, 1997.

[3] M.Milosavljević, G.Grubor, "Osnove bezbednosti i zaštite informacionih sistema", Univerzitet Singidunum, Beograd, 2006.

[4] M.Stamp, "Information Security – Principles and Practice", John Wiley & Sons, Wiley-Interscience, 2006.

[5] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, vol. 28–4, pp. 656–715, 1949, http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf

[6] G.S.Vernam, "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications", Journal of the IEEE, Vol 55, pp109-115, 1926.

[7] S.W. Golomb, *Shift Register Sequences*, Aegean Park Press, 1982.

[8] N.G. de Bruijn, "Acknowledgement of Priority to C. Flye Sainte-Marie on the counting of circular arrangements of 2^n zeros and ones that show each n-letter word exactly once", T.H.-Report 75-WSK-06, Technological University Eindhoven, 1975.

[9] J. L. Massey, "Shift-register synthesis and BCH decoding", *IEEE Trans. Information Theory* **IT-15** (1): 122–127, 1969., http://crypto.stanford.edu/~mironov/cs359/massey.pdf

[10] EFF DES cracker project, http://www.eff.org/Privacy/Crypto_misc/DESCracker/

[11] B. Schneier, *Applied Cryptography*, second edition, Wiley, 1996.

[12] AES algorithm (Rijndael) information, at http://csrc.nist.gov/CryptoToolkit/aes/rijndael/

[13] V. Rijmen, The Rijndael page, at http://www.iaik.tu-graz.ac.at/research/knypto/AES/old/~rijmen/rijndael/

[14] R. Rivest, A. Shamir, L. Adleman. „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". *Communications of the ACM*, Vol. 21 (2), pp.120–126. 1978.

[15] T. El Gamal "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms". *IEEE Transactions on Information Theory* **31** (4): 469-472. 1985.

[16] W. Diffie and M. E. Hellman New Directions in Cryptography, *IEEE Transactions on Information Theory*, vol. IT-22, Nov. 1976, pp: 644–654.

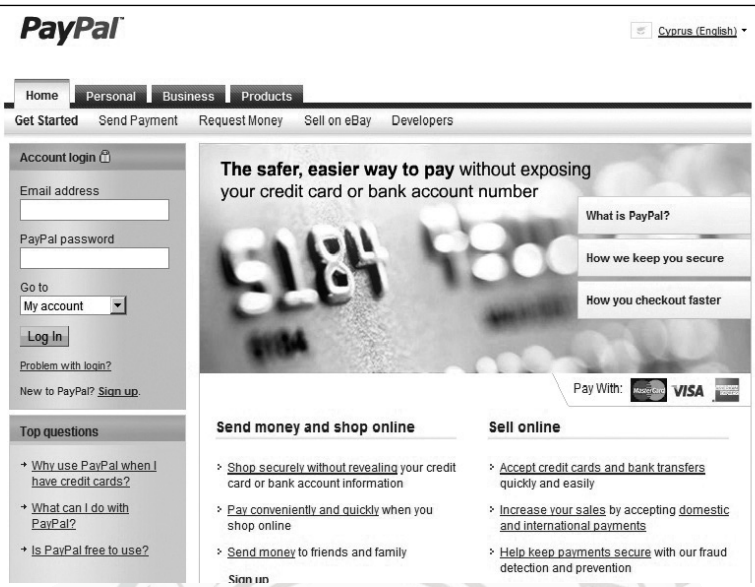
UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

6. PLATNI SISTEMI U E-TRGOVINI

6.1 UVOD

Peter Theil je sedeo sa prijateljima u restoranu. Kada je stigao račun, Theil je izvadio svoj Palm Pilot kako bi podelio iznos sa prijateljem koji je sedeo preko puta njega. Bilo je to u novembru 1999. godine. Theil i njegov ortak, suosnivač, Max Levchin, napravili su sistem pomoću koga mogu da šalju novac jedan drugom preko infracrvenih linkova na Palm Pilot-u. Iz ove ideje se razvio jedan od prvih peer-to-peer platnih sistema PayPal, preko koga je moguće slati novac e-mejlom.

PayPal je lak za korišćenje, kako za one koji šalju, tako i za one koji primaju novac [1]. Prvi korak je kreiranje PayPal naloga na Web sajtu PayPal-a, tako što se popuni formular na kome se daju podaci o kreditnoj kartici ili računu u banci. Samo PayPal ima pristup ovim informacijama, a ne i strana koja prima novac. Kada se koristi PayPal za plaćanje onoga što je kupljeno, novac se prenosi sa kreditne kartice ili bankovnog računa kupca na Automated Clearing House (ACH) mrežu, koja je u stvari privatni finansijski posrednik za praćenje i prenos novca između finansijskih institucija. Strana koja treba da primi novac dobija e-mejl u kome se saopštava da očekuje novac. Ako strana koja treba da primi novac ima nalog na PayPal-u, novac se automatski prenosi na račun. Ako osoba nema PayPal nalog, neophodno je da ga kreira. Nakon toga novac se transferuje na taj račun. Kada novac stigne na PayPal nalog, primalac može da prenese novac elektronskim putem na račun, zatraži ček ili koristi PayPal da bi poslao novac nekom drugom.



Sl.6.1.1. Izgled prve stranice Web sajta PayPal.com

Levchin i Theil su koncipirali PayPal kao metod plaćanja između osoba koje se poznaju. Brzo su shvatili da bi to funkcionisalo i sa kompanijama kao što je eBay, pružajući kupcima i prodavcima način da lakše i brže kupuju, čime bi se izbegavao mučan proces slanja čekova i naloga i čekanja da se čekovi realizuju pre nego što se roba pošalje kupcu. Danas je PayPal najveći i najpopularniji onlajn platni sistem, koji je u početku svog osnivanja 1999. godine imao nekoliko korisnika, a u avgustu 2001. godine je imao 9 miliona korisnika. Krajem 2009. godine PayPal je imao preko 78 miliona aktivnih korisnika u 190 zemalja sa 19 različitih valutnih sistema. Godišnji rast se već duži niz godina održava na nivou od 20%. Web sajt ove kompanije je samo u 2008. godini posetilo više od 260 miliona korisnika. Od 100 prvih onlajn kompanija, čak 44 nude opciju plaćanja preko ovog sistema [2].

PayPal je jedan od najvećih uspeha u e-trgovini. Novac zarađuje na dva načina. Prvo, onlajn prodavci, koji mogu biti ili fizička lica ili mala preduzeća koja ne žele poteškoće ili visoke cene vezane za dobijanje naloga trgovačke kreditne kartice, plaćaju nisku cenu za uslugu, svega 0.29% od transakcije, što je višestruko niže u odnosu na cenu trasakcije preko kreditnih kartica. Potrošači ne plaćaju ništa za korišćenje naloga. Drugo, PayPal zarađuje novac tako što dobija kamatu na osnovu sredstava koja još nisu prenesena sa PayPal sistema.

Snaga PayPal-a leži delimično u njegovoj jednostavnosti: oslanja se na postojeći platni sistem kreditnih kartica i čekova. Ipak, to je i jedna od njegovih slabosti. PayPal ima visok stepen prevara koje imaju veze sa sistemom kreditnih kartica na koji se oslanja. Da bi se zaštitio od prevara, PayPal traži specijalnu dozvolu za iznose od preko $200.

U ovom poglavlju biće reči o postojećim platnim sistemima, prepoznaćemo univerzalne karakteristike ovih sistema, opisaćemo sadašnje i buduće platne sisteme e-trgovine, kako u B2C, tako i u B2B polju.

6.2 PLATNI SISTEMI

Da bismo shvatili platne sisteme u e-trgovini, potrebno je da se upoznamo sa raznim tipovima opštih platnih sistema. Nakon toga će nam biti jasnije potrebe koje moraju da zadovolje platni sistemi e-trgovine moraju, koje ujedno možemo samtrati i kao šansu i izazov koje nudi tehnologija e-trgovine za razvoj novih vrsta platnih sistema.

Postoji pet glavnih vrsta platnih sistema: keš, čekovi, kreditne kartice, nagomilana vrednost i akumulirajući bilans [3].

Gotovina je zakonito sredstvo plaćanja definisano od strane nacionalnih vlasti koji reprezentuje vrednost i to je najraširenij način plaćanja što se tiče broja transakcija videti, sliku 6.2.1. Najvažnija karakteristika gotovine je to što je odmah konvertibilna u druge oblike vrednosti i to bez posredništva bilo koje druge institucije. Na primer, besplatne sakupljanje milja u avionskom saobraćaju nisu izražene u gotovini, jer nisu odmah konvertibilne u druge forme vrednosti – potrebno je posredništvo treće strane, avionske kompanije, kako bi bile zamenjene za vrednost - avionsku kartu. Privatne organizacije ponekad kreiraju formu privatne gotovine koja se naziva *scrip* i koja može odmah biti isplaćena učešćem organizacija svojim dobrima ili kešom. Postoje, na primer, zelene nalepnice ili neki drugi vidovi kupona pomoću kojih se iskazuje lojalnost kupaca.

Sl.6.2.1 Udeo platnog prometa u SAD prema broju transakcija

75% platnog prometa u SAD-u smislu broja transakcija je obavljeno u gotovini ili personalnim čekovima. Zašto je gotovina i dalje toliko popularna danas? Novac u gotovini može da se nosi sa sobom i onaj ko ga poseduje, ima trenutnu kupovnu moć. Gotovina omogućava *mikroplaćanja*, tj. plaćanje malih novčanih iznosa. Korišćenje gotovine je oslobođeno od raznih poreza na transakcije i to od strane i kupca i prodavca. Korišćenje gotovine ne zahteva nikakve dodatnu opremu, kao što su specijalni hardveri ili postojanje nekog računa, a od korisnika se ne traži skoro ništa. Gotovina je anonimna i skoro je nemoguće ući u trag transakcijama obavljenim u gotovini. Stoga je gotovina u tom pogledu popuno privatna. Drugi načini plaćanja zahtevaju značajnu upotrebu trećih lica i ostavljaju za sobom digitalni trag.

S druge strane, gotovina je po pravilu limitirana na manje transakcije, lako ju je ukrasti i uopšte ne obezbeđuje nikakav float - period vremena između kupovine i plaćanja; kada se potroši, nema je više. Što se tiče gotovine, kupovina je konačna i ne može se više izmeniti (ireverzibilnost), sem ako ne postoji drugačiji dogovor sa prodavcem.

Čekovni transferi su sredstva koji se direktno prebacuju preko potpisanog čeka sa čekovnog računa potrošača na prodavca ili drugu osobu. To je drugi najpopularniji način plaćanja u smislu broja transakcija, videti sliku 6.2.1 i najrasprostranjeniji u smislu ukupne vrednosti transakcija, videti sliku 6.2.2.

Čekovi se mogu koristiti i za male i za velike transakcije, izuzimajući jedino mikroplaćanja. Čekovi zahtevaju da prođe određeni period vremena da bi se realizovao, a na nepotrošeni iznos teče kamata. Čekovi nisu anonimni i da bi funkcionisali, potrebno je učešce treće strane, odnosno institucije. Čekovima je lakše izvesti prevaru nego gotovinom. Stoga se prilikom obavljanja čekovnih transakcija zahteva identifikacija izdavaoca čeka. Za prodavca, ček predstavlja i izvestan rizik u odnosu na gotovinu, jer mogu biti stornirani pre izvršene transakcije sa računa ili mogu biti stornirani ako nema dovoljno novca na računu.

Sl.6.2.2 Udeo platnog prometa u SAD prema ukupnoj vrednosti transakcija transakcija.

Nalozi za isplatu, čekovi i putni čekovi su *osigurani* čekovi koji imaju neke limite personalnih čekova. Osigurani čekovi smanjuju rizik bezbednosti personalnog čeka tako što zahtevaju direktno plaćanje poverilačkoj trećoj strani – banci ili kompaniji za transfer novca kao sto je American Express, Wells Fargo ili Western Union. Ove institucije, zatim, izdaju garantovanu isplatu koja se naziva *nalog za isplatu* koji je isto toliko dobar kao i gotovina, mada manje anoniman. Prodavcima je garantovana isplata u bilo kojoj transakciji sa osiguranim čekom. Što se tiče ovih trećih strana, one zarađuju novac tako što potrošačima naplaćuju određenu taksu i dobijaju kamatu na novac koji je potrošač deponovao kod njih. Osigurani čekovi obezbeđuju prodavcima manje rizika, ali potrošači zato plaćaju više. Za uzvrat, potrošači imaju platni instrument koji je skoro svuda prihvaćen i u nekim slučajevima je osiguran protiv gubitaka.

Kreditna kartica predstavlja račun koji pruža potrošačima mogućnost kreditiranja. Udruženja kreditnih kartica kao što su, na primer, Visa i MasterCard su neprofitabilne organizacije koje postavljaju standarde za banke koje izdaju kreditne kartice i vrše transakcije. Ostale treće strane, kao što su procesni centri, proveravaju račune i bilanse. Banke koje izdaju kreditne kartice ponašaju se kao finansijski posrednici koji minimiziraju rizik stranama koje učestvuju u transakciji.

Kreditne kartice omogućavaju potrošačima kredite i mogućnost da kupuju odmah na malo ili veliko. One su uveliko prihvaćene kao platežno sredstvo, smanjuju rizik krađe koji postoji kod nošenja gotovine. Kreditnom karticom, na primer, potrošač može sada da kupi nešto, i da plati tek kad za 30 dana dobije račun. Potrošači profitiraju tako sto ljudi kupuju više uz pomoć kreditne kartice, ali zato plaćaju bankama od 3% do 5% od cene onoga što je kupljeno. Po pravilu rizik transakcije (kao sto su na primer prevare kreditnom karticom, odbijanje transakcije ili neplaćanje) usmerava se na prodavca ili na banku koja izdaje kreditnu karticu. Kada se prijavi nestanak kreditne kartice, imalac nije odgovoran ni za kakve dodatne troškove nastale po osnovu daljeg nelegalnog korišćenja ukradene kartice.

Depozitni računi su nastala od deponovanja sredstava na dati račun. Sa depozitnih računa se mogu vršiti plaćanju ili neki drugi transferi. Ovo platežno sredstvo je slično čekovnim transferima ali ne zahteva ispisivanje čekova. Kao primer navodimo debitne kartice, poklon sertifikate, kartice za avansna plaćanja i smart. Debitne kartice liče na kreditne kartice, ali one ne omogućavaju kredit, već se sa njih odmah skidaju sredstva koja su utrošena u kupovini. Pošto debitne kartice zavise od novčanih sredstava koja se nalaze na računu potrošača, za veće kupovine se, ipak, i dalje koriste kreditne kartice. Peer-to-peer (P2P) platni sistemi, kao sto je PayPal, varijacije su koncepta deponovanih vrednosti. P2P sistemi ne insistiraju na predplaćenosti, ali zahtevaju račun sa deponovanim sredstvima ili čekovni račun sa odgovarajućim sredstvima ili kreditnu karticu sa kreditnim bilansom.

Akumulirani bilansi su računi koji akumuliraju sredstva i na koja potrošači s vremena na vreme uplaćuju sredstva. U tradicionalne primere spadaju telefonski računi ili računi American Express-a. Svi oni akumuliraju bilanse, obično u okviru određenog perioda

(na primer na mesec dana) i onda se isplaćuju u celosti na kraju tog perioda. Tabela 6.2.1 ukratko opisuje kako se platni sistemi mogu karakterisati skupom distinktnih obeležja - dimenzija. Tabela 6.2.1 pokazuje i koliko je preduzetnicima teško da procene nove platne mehanizme i uporede ih sa postojećim platnim sistemima (gotovina, čekovi i kreditne kartice). Kako ćemo kasnije videti, potrošaci u SAD-u nisu, generalno gledajući, prihvatili većinu platnih sistema koji se obavljaju onlajn. Tabela 6.2.1 takođe pokazuje da različite strane koje imaju neki interes u tim platnim sistemima (stakeholders) imaju svoje preference u pogledu pojedinih dimenzija. Najveći stejkholderi u platnim sistemima su potrošači, prodavci, finansijski posrednici i vladini zakonodavci.

Ono što potrošače najviše zanima kod platnih sistema je što manji rizik, niske cene, pouzdanost i raspoloživost. Praksa pokazuje da potrošači ne prihvataju nove platne sisteme ukoliko oni nisu pouzdani barem kao postojeći platni sistemi. Gledno u globalu, velika većina potrošača koristi uglavnom gotovinu, čekove i/ili kreditne kartice. Izbor platnog sistem zavisi od specifičnosti transakcija koje se obavljaju. Na primer, gotovina je možda bolja ako potrošač želi da ostane anoniman i ukoliko želi da sakrije svoje transakcije od javnosti Međutim, ako prilikom kupovine nekog specifičnog proizvoda, npr. automobila, potrošač upravo želi da ostavi trag transakcije, tada sigurno neće koristiti gotovinu nego neko drugo neanonimno platežno sredstvo.

Ono što prodavce najviše zanima jeste niska stopa rizika, niski troškovi, sigurnost i pouzdanost platnog sistema. Trenutno, prodavci se suočavaju sa visokim rizikom u domenu čekova i kreditnih kartica, budući da u tom sektoru ima dosta prevara. Prodavci preferiraju plaćanje gotovinom, čekovima, a manje plaćanje kreditnom karticom, koje po pravilu nose sa sobom visoke takse uz mogućnost odbijanja transakcije nakon izvršene kupovine. Finansijski posrednici, kao sto su banke i mreže kreditnih kartica, najviše su zainteresovani za sigurne platne sisteme koji prebacuju rizik transakcija i troškove na kupce i prodavce, uz maksimizaciju svojih marži. Država je zainteresovana za održavanje poverenja u finansijski sistem. Stoga se kroz odgovarajuću zakonsku regulativu vrši zaštita platnog sistem od raznih upada i prevara, uz nastojanje da interesi kupaca i prodavaca budu izbalansirani, nasuprot jednostranim interesima finansijskih posrednika.

Tabela 6.2.1 Dimenzije platnih sistema

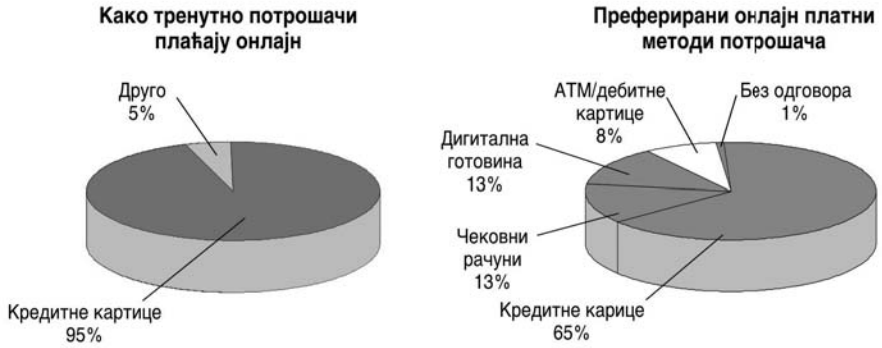
DIMENZIJA	GOTOVINA	PERSONALNI ČEK	KREDITNA KARTICA	DEBITNA KARTICA	AKUMULI-RANI BILANS
Odmah konevrtibilan bez posrednika	da	ne	ne	ne	ne
Mali trošak transakcije za male transakcije	da	ne	ne	ne	da
Mali trošak transakcije za velike transakcije	ne	da	da	da	da
Niski fiksni troškovi za prodavca	da	da	ne	ne	ne
Transakcije koje mogu biti odbijene	ne	da	da	ne (uglavnom)	da
Finansijski rizik za potrošača	da	ne	do $50	ograničen	ne
Finansijski rizik za prodavca	ne	da	da	ne	da
Anonimno za potrošača	da	ne	ne	ne	ne
Anonimno za prodavca	da	ne	ne	ne	ne
Odmah se može potrošiti	da	ne	ne	ne	ne
Bezbednost od nedozvoljenog korišćenja	ne	ponekad	ponekad	ponekad	ponekad
Otpornost na prevare	na	ne	da	da	da
Potrebna je identifikacija vlasnika	ne	da	da	da	da
Potreban poseban hardver	ne	ne	da (od strane prodavca)	da (od strane prodavca)	da (od strane prodavca)
Kupac zadržava "float"- vremenski period od kupovine do plaćanja	ne	da	da	ne	da
Potreban račun	ne	da	da	da	da
Ima trenutnu vrednost novca	da	ne	ne	da	ne

6.3 PREGLED POSTOJEĆIH PLATNIH SISTEMA U E-TRGOVINI

Nastankom e-trgovine stvorile su se nove potrebe finansijske prirode koje u mnogim slučajevima ne mogu biti ispunjene uz pomoć tradicionalnih platnih sistema. Na primer, nove vrste odnosa u kupovini kao što su onlajn aukcije koje se odvijaju između nekoliko osoba, nastale su iz potrebe za metodom peer-to-peer plaćanja uz pomoć kojih učesnici u nekoj trgovinskoj transakciji mogu e-mail-om slati novčane iznose jedni drugima. Nove vrste onlajn informacionih proizvoda zahtevaju mikroplaćanja. Prodavci žele da prodaju onlajn proizvode kao što su individualne muzičke kasete, stubci iz novina i odlomci iz knjiga. Tehnologija e-trgovine nudi zauzvrat veliki broj mogućnosti za stvaranje novih platnih sistema koji će zameniti postojeće sisteme, kao i za stvaranje poboljšanja za postojeće sisteme.

Kreditne kartice čine 95% plaćanja onlajn u SAD-u, videti sliku 6.3.1. Dok su kreditne kartice dominantan način za plaćanja onlajn u SAD-u, ovo ne važi za ostale delove sveta. Van SAD-a samo 50% potrošača koristi kreditnu karticu za kupovinu onlajn. Potrošači u Evropi se više oslanjaju na čekove ili na plaćanja pouzećem. Potrošači u Japanu se oslanjaju na transfere preko banaka, plaćanja pouzećem koristeći lokalne prodavnice kao mesta odakle se preuzima roba i računima akumuliranih bilansa sa telefonskom kompanijom.

U SAD-u je dominacija kreditnih kartica u onlajn kupovini u opasnosti od nastanka novih formi elektronskog plaćanja. Najbrži rast u platnim sistemima je kategorija "Drugo" koja je prikazana na slici 6.3.1 [4].



Slika 6.3.1 Sadašnji najpopularniji metodi onlajn plaćanja

Navedimo neke nove platne sisteme prilagođene digitalnoj ekonomiji:

- Digitalna gotovina: sistemi koji stvaraju privatni oblik monete koja može biti potrošena u okviru sajtova e-trgovine.

- Onlajn sistem akumuliranih vrednosti: sistemi koji se oslanjaju na pretplatu, debitne kartice ili čekovne račune kako bi se stvorila monetarna vrednost koja se može koristiti pri kupovini u e-trgovini.
- Platni sistem digitalnih akumuliranih bilansa: sistemi koji akumuliraju male naplate i periodično naplaćuju svojim potrošačima. Ovi sistemi su naročito pogodni za mikroplaćanja za digitalne sadržaje.
- Digitalni kreditni računi: sistemi koji proširuju onlajn funkcionalnost postojećih platnih sistema kreditnih kartica.
- Digitalni čekovi: sistemi koji stvaraju digitalne čekove za e-trgovinu i proširuju funkcionalnost postojećih čekovnih sistema u bankama.

6.4 TRANSAKCIJE KREDITNIM KARTICAMA U E-TRGOVINI

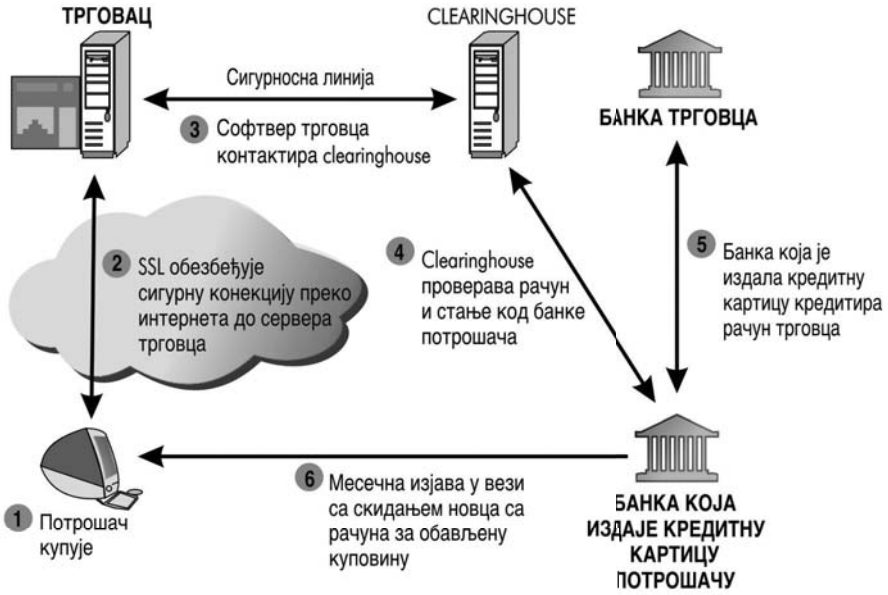
Pošto su kreditne kartice dominantni način onlajn plaćanja, važno je shvatiti kako funkcionišu onlajn transakcije kreditnim karticama i prepoznati slabosti i dobre strane ovog platnog sistema.

Onlajn transakcije kreditnom karticom obavljaju se naoko isto kao i uobičajena kupovina istom karticom. Međutim velika razlika je u tome što onlajn prodavci nikad ne vide karticu koja se koristi, niti se ona provlači kroz fizički čitač kartica, a rezultujući izveštaj se ne potpisuje. Onlajn transakcije kreditnom karticom najviše liče na transakcije vezane za narudžbine poštom ili telefonom. Ovakav tip kupovine se naziva i CNP (Card Not Present – kartica nije prisutna) transakcije i one su najveći razlog zašto naplate mogu kasnije biti predmet odbijanja od strane potrošača. Posto prodavac nikada ne vidi kreditnu karticu, niti dobije od kupca potpis, kada se pojavi neka rasprava, prodavac rizikuje to da transakcija bude onemogućena i odbijena, iako je prodavac već poslao prodatu robu ili je korisnik skinuo sa mreže digitalni proizvod.

Slika 6.4.1 pokazuje ciklus onlajn kupovine kreditnom karticom [5]. U toj kupovini uključeno je pet strana: potrošač, prodavac, klirinška kuća (clearinghouse), banka prodavca i banka koja je izdala karticu potrošaču. Kako bi primio plaćanja kreditnom karticom, prodavac mora imati svoj račun kod banke ili neke finansijske institucije. Račun prodavca je račun u banci pomoću kojeg kompanije mogu obraditi kreditnu karticu i dobiti novac od te transakcije.

Kako je prikazano u slici 6.4.1, onlajn transakcija kreditnom karticom počinje kupovinom (#1). Kada potrošač želi nešto da kupi, on doda stavku proizvoda u potrošačku korpu na Web sajtu prodavca. Kada potrošač zeli da plati robu koju je kupio, stvara se sigurnosni tunel preko Interneta koristeći SSL (Secure Sockets Layer) protokol. Koristeći šifrovanje, SSL obezbeđuje čitav proces tokom kojeg se podaci o kreditnoj kartici šalju prodavcu i štiti te podatke od upada sa Interneta (#2). SSL ne identifikuje ni prodavca ni potrošača. Obe strane moraju imati poverenja jedna u drugu.

Kada prodavac primi informaciju o kreditnoj kartici potrošača, softver prodavca kontaktira klirinšku kuću (clearinghouse) (#3). Klirinška kuća (clearinghouse) je finansijski posrednik koji identifikuje kreditnu karticu i proverava bilans na računu. Klirinška kuća kontaktira banku koja je izdala kreditnu karticu da bi ona potom proverila račun (#4). Kada je kartica proverena, banka koja je izdala kreditnu karticu vrši transfer na račun prodavca u njegovoj banci (#5). Zatim se potrošaču šalje informacija o kupovini (#6).



Sl.6.4.1. Informacioni tokovi prilikom kompletiranja online transakcije kreditnom karticom.

Kompanije koje imaju račun moraju da izgrade ili kupe odgovarajuće sisteme koji omogućavaju kompletiranje onlajn transakcija. Zaštita prodavčevog računa je samo jedan korak u procesu koji ima dva koraka. Danas Internet provajderi platnih sistema obezbeđuju i prodavčev računa i odgovarajući softver za izvršavanje ttransakcija prilikom onlajn kupovine kreditnom karticom.

Na primer, VeriSign, lider u obezbeđivanju servisa zaštite na Internetu, je istovremeno i provajder servisa plaćanja na Internetu. VeriSign pomaže prodavcu da zaštiti svoj račun uz pomoć jednog od svojih partnera iz domena zaštite, uz instalaciju svog softverskog rešenja na serveru prodavca u cilju sprovođenja onlajn platnih transakcija. Softver sakuplja podatke o transakciji sa prodavčevog sajta i zatim ih šalje putem "platnih getveja" VeriSign-a kupčevoj banci, uz proveru da li kupac autorizovan za svaku konketnu kupovinu. Na kraju lanca ovih transakcija je prebacivanje novaca na račun prodavca.

Postoji veliki broj ograničenja u postojećem platnom sistemu kreditnih kartica, kao što su bezbednost, rizik koji preuzima prodavac/kupac i socijalna jednakost. Postojeći sistem je dosta slab što se tiče bezbednosti. Ni prodavac, ni kupac nisu dovoljno zaštićeni. Prodavac bi mogao biti neka kriminalna organizacija koja se bavi sakupljanjem brojeva kreditnih kartica, a kupac možda koristi ukradenu karticu. Rizik sa kojim se suočava prodavac je veoma visok: kupci mogu da odbiju da plate iako je roba već poslata ili sadržaj skinut sa Weba. Troškovi za prodavca su takođe visoki – oko 3,5% od kupovine, plus taksa za transakciju od oko 20 do 30 centi po transakciji, plus još neke druge takse. Veliki troškovi čine da se potrošaču ne isplati da prodaje robu na Web-u koja košta manje od $10. Kupovinu individualnih artikala, muzičkih albuma i nekih drugih sitnih stvari je nemoguće obaviti kreditnom karticom.

Kreditne kartice nisu baš demokratsko sredstvo, iako se čini da su veoma liberalne. Milioni mladih ne poseduju kreditne kartice, zajedno sa ostalim koji sebi ne mogu priuštiti kreditnu karticu jer imaju niske prihode. Alternativni platni sistemi prevazilaze većinu ovih ograničenja. Sama industrija kreditnih kartica je pokušala da reši pitanje bezbednosti preko novog standarda Internet protokola koji se zove SET.

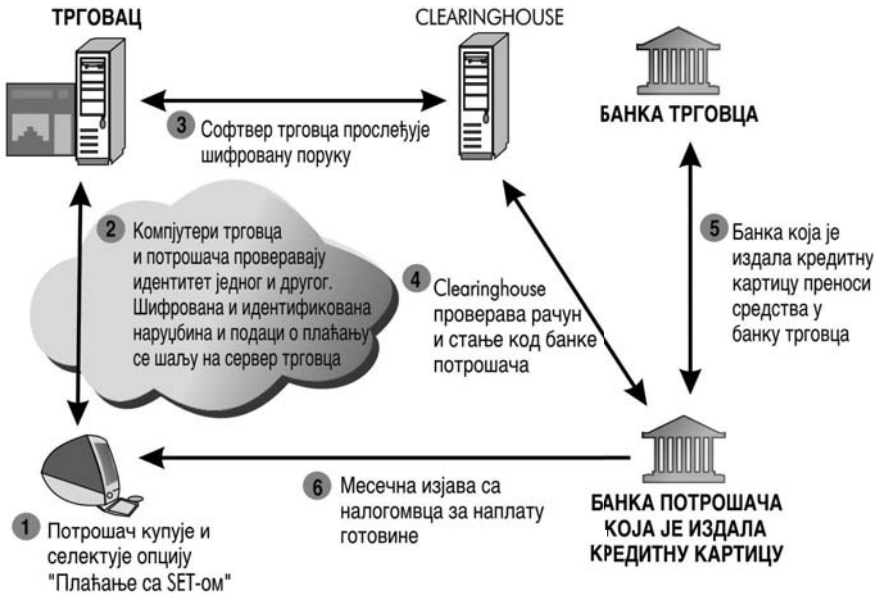
6.5 SET: BEZBEDAN PROTOKOL ZA ELEKTRONSKE TRANSAKCIJE

Centralno pitanje za prodavce i banke koje izdaju kreditne kartice je autentifikacija i odbijanje plaćanja. Iako SSL protokol nudi bezbednu transakciju između prodavca i potrošača, ne obezbeđuje servis autentifikacije. Osim toga, SSL ne može da obezbedi nservis neporecivosti: kupac može da naruči robu ili da skine sa Weba neki sadržaj, a da zatim tvrdi da se ta transakcija nikada nije ni odigrala.

SET koristi *digitalni sertifikat,* o kojem će biti više reči u narednim poglavljina, što je ustvari zakačeni fajl na poruci koji proverava identitet pošiljaoca, kao način da se poboljša bezbednost plaćanja. Kompanije kreditnih kartica izdaju digitalne sertifikate svojim korisnicima kartica istog trenutka kada izdaju i kartice. Digitalni sertifikat se čuva u digitalnom novčaniku, koji će biti podrobnije opisan u narednom odeljku, za upotrebu tokom onlajn transakcija. Prodavcima se izdaju slični sertifikati od strane banke. Upotrebom SET-a, prodavci mogu biti sigurni da prispele narudžbine nisu promenjene tokom celokupnog procesa izvršavanja. SET takođe identifikuje i potrošača i prodavca. Slika 6.5.1 pokazuje kako funkcionišu SET transakcije.

Proces SET transakcije je sam po sebi sličan standardnoj onlajn transakciji u kojoj se koristi kreditna kartica, izuzev toga što ovde ima više verifikacije identiteta. Kao što je prikazano na slici 6.5.1, posle popunjavanja formulara onlajn, potrošač bira opciju ”plaćanje SET-om” i zatim bira kojom će kreditnom karticom platiti (#1). Kada primi

popunjeni formular, računar prodavca pristupa digitalnom novčaniku kupca u cilju prikupljanja podataka o kreditnoj kartici. Server prodavca proverava identitet kupca tako što koristi digitalni sertifikat u okviru digitalnog novčanika, kao što na isti način računar kupca proverava identitet prodavca. Kada je identitet proveren, šalje se šifrovana poruka na server prodavca koja sadrži sve podatke o plaćanju (#2). Zatim server prodavca dalje šalje šifrovanu poruku u banku prodavca kako bi se ova dešifrovala (#3). Clearinghouse dalje identifikuje prodavca i vlasnika kreditne kartice, tako da se transakcija dalje nastavlja kao bila koja druga kupovina kreditnom karticom (#4, #5). Prodavac dobija dozvolu da isporuči robu, proizvod se dalje šalje kupcu i na kraju se sa računa kupca skida novac za tu kupovinu (#6). Napomenimo da će u Poglavlju 10, biti detaljno opisani kriptološki mehanizmi na kojima počiva SET.



Sl.6.5.1. Kako funkcioniše transakcija preko SET-a

6.6 DIGITALNI PLATNI SISTEMI U B2C DOMENU E – TRGOVINE

Tradicionalni platni sistemi nisu dizajnirani za upotrebu u novom digitalnom svetu elektronske trgovine. Porastom upotrebe Interneta i e-trgovine, postaju očigledne slabosti gotovine, čekova, kreditnih i debitnih kartica. Kao rezultat toga, preduzetnici i tradicionalne finansijske institucije stvorili su veliku paletu opcija digitalnog plaćanja koje izlazi u susret i kupcima i prodavcima. Ovde ćemo detaljnije govoriti o najvećim digitalnim platnim sistemima: digitalna gotovina, onlajn platni sistemi akumulirane vrednosti, digitalni platni sistemi akumuliranih bilansa, digitalni platni sistem kreditnih kartica i digitalni platni sistem čekova. Prvo će biti reči o konceptu "digitalnog novčanika" (ponekad nazivan i *elektronski novčanik* ili *e-novčanik*), budući da veliki broj novih digitalnih platnih sistema zahteva neku vrstu digitalnog novčanika.

6.6.1 Digitalni novčanici

Običan "analogni novčanik" se nalazi u džepu ili tašni. Analogni novčanici su univerzalni; skoro svaka civilizacija zasnovana na transakcijama ima neku vrstu portabl magacina za vrednosti i identifikaciono sredstvo. U novčaniku se obično nalaze lična karta, telefonske kartice, kreditne/debitne kartice. Digitalni novčanik pokušava da nadmaši funkcionalnost analognog novčanika [6]. Najvažnije karakteristike digitalnog novčankla su: (a) autentifikacija kupca preko upotrebe digitalnih sertifikata ili drugih metoda šifrovanja, (b) nagomilavaju i transfer vrednosti i (c) obezbeđenje procesa plaćanja od kupca do prodavca.

U scenariju sa digitalnim novčanikom, korisnik može otići onlajn na neki Web sajt, upotrebiti svoj digitalni novčanik za identifikaciju, platiti izabranu robu koristeći nekoliko platnih sistema i to samo jednim klikom. Uz to ova akcija ostavlja za sobom trag o izvršenoj transakciji koji je odmah dostupan za pregledanje. Isti digitalni novčanik može da funkcioniše i na bežičnom Internet uređaju, kao što su mobilni telefon ili Palm računar. Digitalni novčanici podržavaju plaćanja regularnom kreditnom karticom, digitalnom gotovinom, digitalnim kreditnim karticama ili digitalnim čekovima.

Najveća prednost digitalnih novčanika je udobnost kupaca i manji troškovi transakcija. Pojavom digitalnih novčanika, nije potrebno više popunjavanje onlajn formulara u cilju obavljanja kupovine. Umesto toga, klikom na digitalni novčanik automatski se popunjavaju onlajn formulari u vezi formiranja računa i transportne otpremnice, ali i potencijalno smanjuje rizik prevare i upotrebu ukradenih kreditnih kartica. Prodavci profitiraju od digitalnih novčanika preko manjih transakcionih troškova, većih marketinških šansi, lakšeg zadržavanja kupaca, konverzija posetilaca u kupce i smanjivanja verovatnoće prevara. Finansijski posrednici koji izdaju digitalne novčanike profitiraju od taksi za svaku transakciju. Neke od velikih potencijala digitalnih novčanika prikazane su u tabeli 6.6.1.

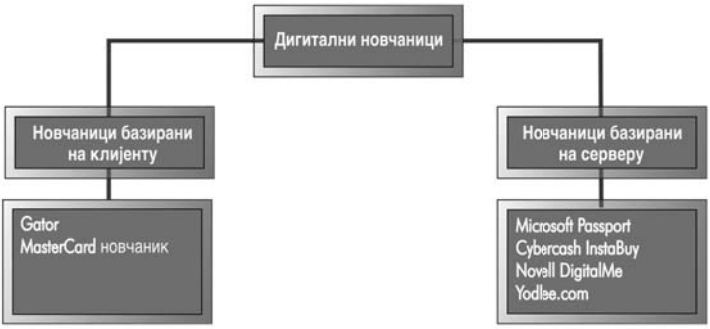
Tabela 6.6.1 Funkcije digitalnih novčanika

FUNKCIJA	OPIS
Autentifikacija	Potvrđuje identitet preko digitalnih sertifikata, SET ili drugih oblika šifrovanja.
Plaćanje	Plaćanje računa preko veza sa bankama koje izdaju kreditne kartice i udruženja.
Privatnost / lozinka	Pomaže kupcima da kontrolišu svoju digitalnu okolinu, PIN-ove, brojeve kartica i lozinke u bezbednom sistemu.
Primanje	Pregled svih transakcija preko jednog izvora.
Prezentovanje računa	Prezentuje i plaća račune sa iste lokacije.
Programi lojalnosti	Učestvuje i upravlja poenima lojalnosti sa iste lokacije.
Isporuka kupona / sniženja	Koordinira promocije prodavca preko jedinstvenog novčanika.
Dozvole	Uspostavlja e-dozvole.
Mikroplaćanja	Plaća sve ispod $5 bilo gde na Web-u, a zasnovano na kreditnoj kartici.
Integracija sa drugim softverom	Povezuje se sa softverom za takse, lične budžete, lične uređaje i bežični softver.

I pored odličnog koncepta, digitalni novčanici ostavljaju dosta važnih pitanja bez odgovora, kao na primer ko će snabdevati digitalne novčanike, ko je vlasnik novčanika i podataka u njemu, gde će biti digitalni novčanik (na desktopu ili nekom udaljenom serveru) i kakvi standardi će definisati digitalni novčanik tako da bude univerzalno prihvaćen.

Trenutno, postoje dve velike kategorije digitalnih novčanika : novčanici bazirani na klijentu i novčanici bazirani na serveru, Sl. 6.6.1.

Digitalni novčanici bazirani na klijentu kao sto je Gator.com i MasterCard Wallet su softverske aplikacije koje kupac instalira na svoj računar [7]. Oni nude kupcima udobnost, tako što se formulari automatski popunjavaju u onlajn prodavnicama. Prodavci instaliraju softver na svoj server, kako bi dobili podatke iz novčanika baziranog na klijentu. Kada kupac klikne relevantno dugme na sajtu prodavca, server prodavca ispituje pretraživač kupca radi podataka o njemu ili o digitalnom novčaniku. Digitalni novčanici bazirani na klijentu imali su do sada malo uspeha.



Sl. 6.6.1. Vrste digitalnih novčanika

Digitalni novčanici bazirani na serveru su imali više uspeha. To su platne usluge i proizvodi koji se prodaju finansijskim institucijama ili direktno ili kao deo paketa njihove finansijske usluge, bazirani na softveru za autentifikaciju. Prodavci mogu ponuditi i tehnološke usluge (infrastruktura koja je potrebna da bi se obavio proces naplate) i usluge novčanika. Trgovci i finansijske institucije koriste proizvode i usluge digitalnog novčanika, kako bi obezbedili laku i bezbednu kupovinu, koristeći metod plaćanja koji izabere sam potrošač. Ovi novčanici nude onlajn trgovcima proizvod/uslugu koji se bavi svim aspektima onlajn plaćanja kupaca, i nudi jeftinije troškove transakcije, manje troškove za potrošača i troškove magacioniranja, kao i odličnu onlajn uslugu plaćanja. Ovi digitalni novčanici ne zahtevaju da potrošač instalira poseban softver i mogu biti lako automatski ažurirani.

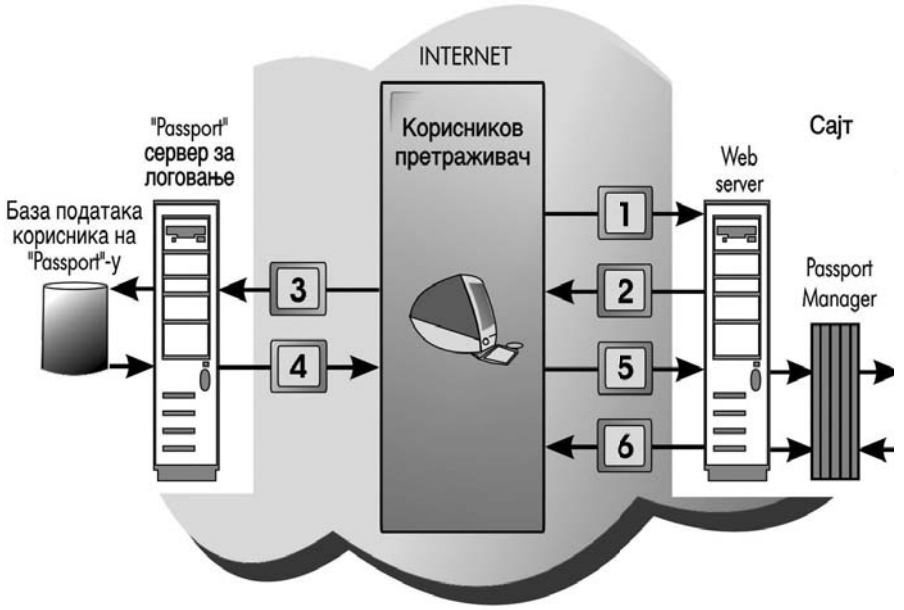
Jedan od najvećih sistem digitalnih novčanika baziranih na serveru je Majkrosoftov Passport (Microsoft's Passport), danas poznatiji kao Windows Live ID [8]. Passport je jedan deo Majkrosoftove .NET platforme i strategije. Passport nudi korisnicima uslugu logovanja (Single Sign-In service SSI), i kao opciju ekspresnu kupovinu (Express Purchase EP). Opcijom SSI-a, korisnik može da se uloguje na Web sajt jednim klikom na logo Passport-a koji se pojavljuje na sajtovima. Isto tako, koristeći EP opciju jednim klikom, potrošač izražava svoje preference što se tiče plaćanja i to se saopštava trgovcu. Dakle, nema više popunjavanja formulara na svakom Web sajtu.

Passport je jedinstven među digitalnim novčanicima, jer nije više potreban digitalni sertifikat. Raniji digitalni novčanici su se oslanjali na digitalne sertifikate, kako bi autentifikovali transakcije između trgovca i klijenta.

Korisnik dobija Passport tako što se nakon otvaranja e-mail računa na MSN.com ili Hotmail.com, registruje na Web sajtu trgovca ili na www.passport.com. Kako bi korisnik dobio svoj jedinstveni profil, mora da da svoje korisničko ime, lozinku i neke opšte po-

datke o sebi. Ova razmena podataka je šifrovana SSL protokolom. Korisnik ima opciju da napravi profil "novčanik" koji sadrži podatke o plaćanju kreditnom karticom koja može biti korišćena od trgovca za EP opciju. Kada se napravi profil, korisniku se daje Passport Unique Identifier (PUID), odnosno jedinstveni passport za identifikaciju od 64-bita. PUID služi za identifikaciju i šalje se trgovcu na njegov sajt kada se Passport korisnik uloguje. Ostali sajtovi nikada ne dobiju lozinku korisnika. Slika 6.6.2 pokazuje šta se dešava kada registrovani korisnik klikne na logo Majkrosoftovog Passport-a.

Kada registrovani korisnik klikne na logo Passport-a na sajtu, pojavi se strana na kojoj korisnik treba da se uloguje, tako što će uneti svoje korisničko ime i svoju lozinku (#1). Strana na kojoj se korisnik loguje se prebacuje na server Majkrosoft Passport-a, kako bi korisnik bio identifikovan (#2, #3). Passport identifikuje korisnika i napravi cookie na korisnikovom pretraživaču koji sadrži šifrovanu identifikaciju i podatke o Passport profilu. Passport menadžer na sajtu dešifruje podatke (#4, #5). Passport menadžer zatim proveri u cookie-ju podatke o korisniku i njegovom Passport profilu i neprimetno ih ponovo proverava, dok se korisnik šeta od strane do strane na Web sajtu (#6). Ekspres plaćanje ima slično ponašanje.



Sl. 6.6.2. Kako funkcioniše Majkrosoftov passport novčanik (Windows live ID)

Po tipičnom poslovnom modelu prodavca baziranom na serveru, proizvod treba direktno staviti kod trgovca i velikih finansijskih posrednika kao što su Visa, MasterCard i Discover Card, i razviti dobar platni sistem i korisničku podršku, kako bi potrošači stekli poverenje i smanjili rizik od zloupotreba kreditnih kartica. Ovi prodavci ukazuju na činjenicu da preko 60% onlajn kupovine kreditnom karticom biva prekidano pre nego sto potrošač potvrdi narudžbinu zbog straha od davanja podataka o kreditnoj kartici. Ovi prodavci su razvili i partnerstvo sa većim udruženjima kreditnih kartica i bankama koje izdaju kreditne kartice, kao što su Wells Fargo, Citibank i Chase, koje traže brza rešenja za zloupotrebe kreditnih kartica i zbunjenost potrošača.

Model prihoda za ove digitalne novčanike bazirane na serveru je da ostvare prihod, tako što će naplatiti trgovcima taksu za instalaciju, minimalne mesečne takse i taksu za svaku transakciju. Neki prodavci prikupljaju podatke o potrošačevoj transakciji i prodaju je drugim marketinškim firmama.

Pokušaji da se naprave standardi za digitalne novčanike su propali. Konzorcijum u čijem su sastavu Dell, AOL, American Express, Sun Microsystems, Brodia, MasterCard, IBM i Microsoft, koji je nastao sa ciljem da se napravi standard nazvan Electronic Commerce Modeling Language (ECML) – elektronski jezik za trgovinu – vrlo je malo napredovao od 1999. godine, iako se Majkrosoftov Passport slaže sa ECML [9]. Druge konkurentske grupe, kao što su Open Trading Protocol (OTP) i Open Buying on the Internet (OBI), su takođe jako malo napredovale.

Imajući u vidu konfliktne platforme koje su usvojili prodavci i jako male beneficije za potrošače koji bi morali da usvoje veliki broj različitih digitalnih novčanika kako bi efikasno kupovali onlajn, jasno pokazuje da je potrebno da prođe još mnogo godina kako bi se vizija o digitalnim novčanicima ispunila.

6.6.2. Digitalna gotovina

Digitalna gotovina ili *e-gotovina* bila je jedna od prvih alternativnih platnih sistema nastalih za potrebe e-trgovine. Naziv digitalna gotovina je pomalo pogrešan naziv. Definicije gotovine je da je to zakonsko sredstvo plaćanja, tj. novac, definisan od strane nacionalnih vlasti i koji je konvertibilan u druge vrste dobara i usluga bez posredstva trećeg lica. Do danas, ni jedna zemlja, nije uspela da stvori elektronsku formu novca kao zakonskog sredstva plaćanja. Umesto toga, ono što dans imamo je neka zanimljiva vrsta sakupljanja vrednosti i razmene vrednosti koje imaju ograničenu konvertibilnost u druge vrste vrednosti i za koje su potrebni posrednici prilikom konverzije. Iako su raniji primeri digitalne gotovine pretrpeli poraz, veliki broj ideja je do danas preživeo kao deo P2P (peer-to-peer) platnih sistema. Tabela 6.6.2 pokazuje neke primere digitalne gotovine.

Tabela 6.6.2 Primer digitalne gotovine

IME SISTEMA	GODINA OSNIVANJA / OPIS
First Virtual	1994. Prvi sigurni sistem deponovane vrednosti zasnovan na kreditnim karticama, depozitima i PIN brojevima. Operacije prestale 1998. god.
DigiCash (sada e-cash)	1995. Pripejd šifrovani sistem deponovane vrednosti koji zahteva digitalnu gotovinu na hard disku. Operacije prestale 1998. god., vratio se kao e-cash.
Millicent	1995. Ulazak u mikroplaćanja e-gotovinom (Digital Equipment Corporation). Sada Compaq platforma proizvoda sa velikim brojem opcija.
PEER-TO-PEER PLATNI SISTEMI	
PayPal	1999. Besplatni P2P sistem mikroplaćanja.
Yahoo PayDirect	1999. Besplatna Yahoo P2P platna usluga.
MoneyZap	1999. Besplatni sistem za transfer novca Western Union

Ranije generacije digitalne gotovine bile su kompleksne i zahtevale su nove sisteme standarda platne industrije. Na primer, Slika 6.5.3. daje opis funkcionisanja DigiCash-a, prve generacije platnog sistema digitalne gotovine.

Kako vidimo na slici 6.6.3. da bi kupac koristio DigiCash, prvo mora da otvori račun u banci koja koristi DigiCash sistem (#1). Nakon toga, potrošač mora da skine sa Interneta na hard disk svog računara softver za digitalni novčanik (#2). Zatim, kupac može da zatraži transfer digitalne gotovine (#3, #4). Čim se gotovina nađe u digitalnom novčaniku, kupac može da troši taj novac kod trgovaca koji su voljni da ga prime (#5). Softver bi uzeo gotovinu iz digitalnog novčanika i preneo ga kod trgovca. Trgovac, zatim, može da prenese novac nazad u banku, kako bi potvrdio da novac nije duplo potrošen (#6). Banka bi onda stornirala e-novčiće i kreditirala račun trgovca u banci (#7).

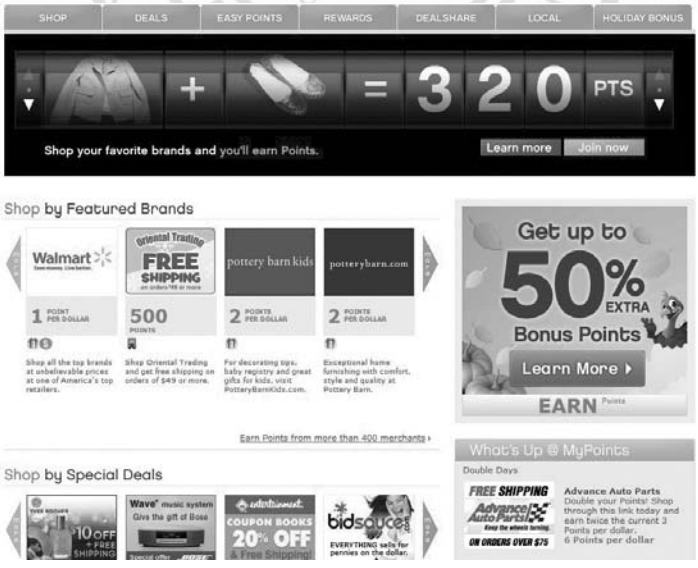
Ovaj prvi koncept nije imao uspeha na tržistu, jer je bio previše komplikovan i za trgovca i za potrošača. Ni DigiCash, ni First Virtual, ne nude više te usluge u onoj formi u kojoj su bile zamišljene.

Razvoj eBay-a, Web sajta onlajn aukcija, stvorio je potrebu za platnim uslugama koje bi omogućile jednostavno plaćanje kupljenih stvari, kao i trgovcima da primaju uplate od kupaca. Osim toga, na tržistu je postojala potreba za uslugom pomoću koje bi se mogli slati mali iznosi novca preko Web-a. Početkom 1998. godine, pojavio se veći broj P2P sistema od kojih je najpopularniji već opisani PayPal. Drugi P2P platni sistemi uključuju Yahoo's PayDirect, AOL's QuickCash, Western Union's MoneyZap i Citibank's C2it.

Kao vid gotovine, PayPal i drugi P2P platni sistemi, imaju određena ograničenja. Sistemi zahtevaju posrednika, a plaćanja se prihvataju samo od onih korisnika koji imaju svoju e-mail adresu.

Sl. 6.6.3. DIGI CACH: Kako je funkcionisala prva generacija digitalne gotovine

Jedna varijacija koncepta digitalne gotovine je gift cash (poklon gotovina), a to je vid e-gotovine u kojoj se zarađuju određeni poeni. Dva najpoznatija provajdera poklon gotovine je Beenz.com, koji poklanja poene za realizovanu kupovinu, i Flooz.com, koji izdaje poklon sertifikate nakon kupovine. Oba provajdera su prestala da rade 2001. godine. MyPoints.com izdaje poene koji mogu biti zamenjeni za robu ili poklon sertifikate, ali ne i gotovinu i još uvek je aktivan. Prva stranica Web sajta ove kompanije prikazana je na sl.6.6.4.



Sl. 6.6.4. Prva stranica Web sajta MyPoints.com, 2010. godina.

6.6.3. Onlajn sistemi akumuliranih vrednosti

Onlajn platni sistemi akumuliranih vrednosti omogućavaju korisnicima da izvrše trenutno onlajn plaćanja. Zasnovani su na vrednostima akumuliranim na onlajn računu. Neki sistemi ove klase zahtevaju od korisnika da skinu sa mreže digitalni novčanik, na primer, Monetta-ova debitna usluga i pripejd usluga eCharge-a, dok drugi zahtevaju od korisnika da se prijave i prenesu novac sa računa na kojima imaju kreditnu karticu, na onlajn račun akumuliranih vrednosti. Ovi sistemi se oslanjaju na akumulirane vrednost u banci kupca, čekovni ili račun za kreditnu karticu. Tabela 6.6.3. opisuje neke od poznatijih sistema akumuliranih vrednosti. Ecount nudi, na primer, pripejd debitni račun. Slika 6.6.5. ilustruje kako funkcioniše Ecount. Da bi se koristio Ecount, korisnik treba da napravi račun kod Ecount-a, i to na bazi kreditne ili debitne kartice. Podaci o računu se šalju preko Weba uz pomoc SSL-a (#). Kada Ecount proveri račun i stanje na njemu kod banke koja je izdala kreditnu karticu korisnika (#2), potrošač može da kupuje bilo gde na Web-u gde je prihvaćen MasterCard (Ecount se tretira kao da je MasterCard), kao i da plaćaju preko e-maila. Primalac mora da se učlani kod Ecount-a da bi mogao da primi novac) (#3). Ecount odmah skida novac sa računa kupca i šalje novac trgovcu (#4). Na kraju meseca, banka koja je kupcu izdala kreditnu karticu, šalje izveštaj o tome da je novac transferisan na Ecount (5#). Na Ecountovom Web sajtu kupac onlajn može da vidi podatke o obavljenoj transakciji.

Rocketcash je još jedna kompanija koja nudi onlajn sistem akumuliranih vrednosti Njena ciljna grupa su adolescenti.

Tabela 6.6.3 Onlajn sistemi akumuliranih vrednosti

IME SISTEMA	GODINA OSNIVANJA/OPIS
Ecount	1998. Pripejd debitni račn
Monetta Prepaid	2000. Pripejd virtualna kartica kojom je moguće kupovati i plaćati onlajn bez kreditne kartice i bankovnog računa. Digitalni novčanik.
Monetta Debit	2000. Račun pomoću kojeg korisnik može da plaća sa postojećeg čekovnog računa ili kreditnih računa. Digitalni novčanik.
eCharge	1997. pripejd račun sa digitalnim novčanikom.
Millicent	1998. Pripejd kartice za kupovinu u prodavnicama (samo u Japanu)
SMART KARTICE	
Mondex	1994. Smart kartica, sistem akumulirane vrednosti, gde se sredstva čuvaju na čipu na kartici.
American Express Blue	1999. Kombinovana kreditna i smart kartica.

Sl. 6.6.5. Kako funkcioniše ECOUNT: Sistem akumuliranih vrednosti

Smart kartice su još jedna vrsta sistema akumuliranih vrednosti koji ima oblik plastične kreditne kartice na kojoj se nalazi čip sa ličnim podacima. Dok klasične kreditne kartice čuvaju na magnetskoj traci samo podatke o jednom broju računa, smart kartice mogu da čuvaju znatno više više podataka, uključujući i nekoliko brojeva kreditnih kartica, podatke o zdravstvenom osiguranju, prevozu, lične podatke, bankovne račune, programe lojalnosti, kao i druge značajne podatke. Ova mogućnost ih čini vrlo atraktivnom alternativom, jer se više ne mora nositi veliki broj pojedinačnih kreditnih kartica i lična karta. Za razliku od običnih kreditnih kartica, pristup smart karticama je moguć samo uz upotrebu lozinke, što je jedan mehanizam više u obezbeđivanju sigurnosti ovih kartica.

Postoje dve vrste smart kartica: kontaktne i nekontaktne, u zavisnosti od tehnologije koja je primenjena. Kontaktne kartice, da bi mogle biti učitane, moraju fizički da se stave u aparat za učitavanje kartica, dok nekontaktne kartice imaju antenu ugrađenu u samu karticu, što omogućava prenos podataka bez direktnog kontakta. Smart kartica, kao što je poklon kartica kupljena za izvesnu sumu je primer kontaktne kartice, jer ona mora da prođe kroz čitač kartica, kako bi plaćanje moglo biti izvršeno. Sistem plaćanja putarine na autoputu, kao što je EZPass je primer nekontaktne smart kartice, čiji sadržaj isčitava udaljeni senzor.

Tehnologiju smart kartice je u početku stvorila francuska mreža javnih govornica, kao pogodan način za plaćanje javnog telefona. One nisu baš opšteprihvaćene u SAD-u zbog masovne tekuće upotrebe kreditnih kartica.

Mondex kartica je jedna od originalnih smart kartica koja je napravljena 1990. godine od strane NatWest Bank u Engleskoj. Kartica sadrži integrisano kolo od 20mm sa CPU od 8 bajtova, brzine 10 MHz i sa 512 KB RAM-a. Lansirana je 1994. godine kao komercijalni proizvod. Ovom karticom korisnik može da skine gotovinu sa bankovnog računa na karticu preko telefona koji je kompatibilan sa Mondex-om ili preko čitača kartice koji je zakačen na PC. Ova kartica može simultano da nosi nekoliko vrsta valuta i mogu je prihvatiti svi trgovaca koji imaju instaliran čitač kartica. Ipak, ova kartica nije doživela komercijalni uspeh.

Zanimanje za smart kartice se unekoliko povećalo u SAD-u od 1999. godine, kada je American Express izbacio svoju smart karticu American Express Blue. Blue je kombinovana kreditna i smart kartica. American Express je napravio specijalni Web sajt za Blue sa kojeg korisnici mogu da skinu digitalni novčanik i tako dobiju posebne usluge, kao što su besplatno onlajn plaćanje računa, zabavnih sadržaj i različitih informacija. Digitalni novčanik omogućava kupovinu jednim klikom i automatsko popunjavanje formulara. Fizički trgovci širom sveta mogu da ubace karticu na prodajnom punktu, baš kao i svaku drugu karticu. Korisnici takođe mogu da čuvaju svoj digitalni novčanik na čipu koji se nalazi na njihovoj kartici. American Express je poklanjao čitače smart kartica koji se priključuje na PC, omogućavajući korisniku da kupuje onlajn na bezbedan, šifrovan način, koji uz to zahteva i identifikaciju korisnika. American Express je distribuirao preko 4 miliona ovih kartica. Oflajn trgovci moraju da instaliraju čitače u svojim prodavnicama, kako bi mogli koristiti smart kartice. Onlajn trgovci su morali da razviju novu infrastrukturu koja bi prihvatila podatke sa čitača kartica kupaca. Trošak oko prelaska američkih trgovaca od kreditne kartice na American Express smart karticu je koštao oko 11 milijardi dolara. Wal-Mart je proračunao da je potrebno oko 10 godina da se sistem koji se koristi u prodavnicama prilagodi tako da mogu da se učitavaju smart kartice. Kao rezultat, imamo da se American Express trenutno koristi prvenstveno kao kreditna kartica, dok njihova smart kartica nije široko prihvaćena među trgovcima i potrošačima.

6.6.4. Digitalni platni sistemi akumuliranih bilansa

Digitalni platni sistemi akumuliranih bilansa omogućavaju korisnicima da izvršavaju mikroplaćanja na Web-u, tako što akumuliraju debitni bilans sa kojeg im se skida novac na kraju meseca. Kao što se plaća telefonski račun na kraju meseca, tako i potrošači moraju da plate ceo iznos na kraju meseca koristeći čekovni ili račun kreditne kartice. Ovaj sistem je idealan za kupovanje intelektualne svojine na Web-u, kao što su muzički CD-ovi, odeljci iz knjiga ili članci iz novina. Tabela 6.6.4 pokazuje neke od ovih sistema.

Jedan od najpoznatijih digitalnih sistema akumuliranih bilansa je qPass [10]. qPass je integrisana platforma za marketing, prodaju, distribuciju i transakcije digitalnih sadržaja. To je vodeće rešenje za mikroplaćanja za medijske kompanije kao što su New York Times, Wall Street Journal i mnoge druge novine i časopise koji pokušavaju da svoj analogni

sadržaj pretvore u digitalni sadržaj u cilju lakše prodaje. Cene su u rasponu od nekoliko centi do nekoliko hiljada dolara. Trenutno qPass ima preko 500 000 registrovanih korisnika.

Da bi koristili qPass, korisnici moraju da skinu sa Interneta digitalni novčanik koji šifruje i identifikuje njihove transakcije. Ove transakcije ne mogu biti opozvane od strane korisnika. Kada je digitalni novčanik instaliran, kupci mogu da kupuju digitalne sadržaje na Web sajtovima e-trgovine. Kupci plaćaju ovaj digitalni sadržaj tako što kliknu na qPass prozor na sajtu. Na kraju meseca, qPass naplaćuje sumu sa korisnikove kreditne kartice ili nekog drugog računa.

iPIN je nov na tržištu mikroplaćanja akumuliranih bilansa. iPIN pruža usluge ili kao provajder aplikativnog softvera, ili kao rešenje na strani trgovca. Sa iPIN-om, kupac može da bira nivo bezbednosti i identifikacije, od jednostavnog logovanja sa korisničkim imenom i lozinkom do digitalnog novčanika. iPIN se oslanja na postojeće platne usluge, kao na primer za telefon, bežični pristup Internetu ili bankovne račune u cilju izdavanja i naplate računa. Ove usluge su postale konkurentne za kupovine manje od 20 dolara. Široko su prihvaćene na muzičkim Web sajtovima koji prodaju muzičke albume za 99 centi.

Tabela 6.6.4 Digitalni platni sistem akumuliranih bilansa

SISTEM	GODINA OSNIVANJA/OPIS
QPass	1997. Integrisana platforma za mikroplaćanja koja cilja na provajdere digitalnih sadržaja. Koristi se digitalni novčanik.
iPIN	1997. Integrisana platforma sa akumuliranim bilansima i fleksibilnim procedurama identifikacije.
Millicent	1998. Compaq platforma optimizirana za kupovinu i prodaju digitalnih sadržaja. Korisnici mogu da otvore račune preko ISP-a, telefona ili nekog drugog sistema plaćanja [14].

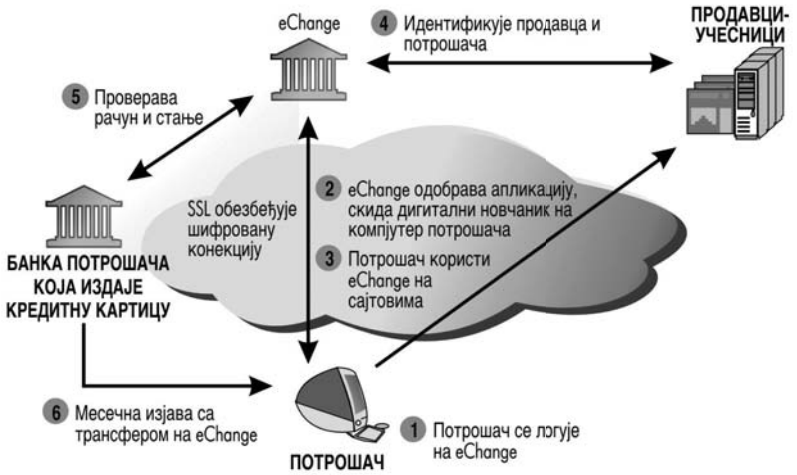
6.6.5. Digitalni platni sistemi preko kreditnih kartica

Digitalni platni sistemi preko kreditnih kartica pokušavaju da prošire svoju delatnost postojećih kreditnih kartica kao sredstva za onlajn kupovine. Iako mnogi, ako ne i svi novi digitalni platni sistemi, koriste postojeću platnu čekovnu i kreditnu infrastrukturu, digitalni platni sistem preko kreditnih kartica je fokusiran na bezbednije korišćenje kreditnih kartica, što je povoljnije i za kupca i za prodavca. Ovi sistemi pokušavaju da reše ozbiljna ograničenja onlajn plaćanja kreditnom karticom, kao što su nedostatak identifikacije, odbijanje plaćanja i zloupotreba kreditnih kartica. Ovi sistemi pokušavaju da reše i konstantni problem straha potrošača od davanja delikatnih podataka na Web sajtovima na Internetu. Takođe pokušavaju i da smanje troškove transakcija, tako što su uveli automatsko popunjavanje formulara. Tabela 6.6.5 prikazuje neke od digitalnih platnih sistema preko kreditne kartice.

Tabela 6.6.5 Digitalni platni sistemi preko kreditnih kartica

SISTEM	GODINA OSNIVANJA/OPIS
eChargeCredit	1997. eCharge omogućava korisnicima da prenesu svoja onlajn plaćanja na račune kreditnih kartica. Mora da se skine sa mreže digitalni novčanik.
BillPoint Online Payments	1995/98. Ulazak eBay-a, WellsFargo-a i Visa-e u P2P platni sistem. BillPoint omogućava prodavcima sa eBay-a da prihvate plaćanja kreditnom karticom kupaca, a da nije neophodno da imaju račun kod trgovca. Nije potreban digitalni novčanik.

eCharge je kreditni digitalni platni sistem koji koristi digitalni novčanik baziran na klijentu. Kao što je prikazano na slici 6.6.6, korisnik se uloguje na račun eCharge-a, prosleđuje podatke o računu kreditne kartice eCharge-u preko SSL šifrovane bezbedne konekcije (#1). Pošto odobri potrošačevu aplikaciju, eCharge skine na korisnikov računar digitalni novčanik (#2). Potrošač dalje može da kupuje na svim sajtovima koji prihvataju eCharge kao platnu opciju (#3). eCharge, zatim, identifikuje i prodavca i kupca, tako što verifikuje njihove digitalne sertifikate (#4), kupčev račun i bilans kod banke potrošača (#5), i onda autorizuje transakciju. Kupci plaćaju svoj račun elektronskim putem, svakog meseca preko postojećeg kreditnog ili debitnog računa, bilo kog bankovnog računa ili eCharge telefona, ili bilo kojeg naplatnog telefonskog sistema (#6).



Sl. 6.6.6. Kako funkcioniše digitalni platni sistem preko kreditne kartice eCharge

BillPoint je digitalni platni sistem preko kreditne kartice koji omogućava kupcima i prodavcima na malo koji koriste eBay, da prihvate plaćanja preko kreditne kartice bez troškova prilagođavanja servera i softvera prodavca ili računa prodavca kod banke koja izdaje kreditnu karticu. U suštini, eBay i BillPoint postaju banka kod koje je račun prodavca i naplaćuju od prodavaca taksu za procesiranje svake transakcije u iznosu od 4,5%, plus 75. BillPoint nudi kupcima ostavljanje traga iza svake kupovine.

American Express i Discover nude varijaciju na tradicionalne kreditne kartice, kako bi smanjili strah potrošača od zloupotrebe i krađe preko kreditnih kartica. Private payments American Express-a i deskshop Discover-a omogućavaju vlasnicima kartica da naprave "virtuelnu" kreditnu karticu na bazi novog broja računa koji se vezuje za pravi broj računa. Taj broj može biti korišćen samo jedanput, tako da kada se jednom upotrebi, ne može biti ukraden ili zloupotrebljen. Ipak, potrošači nisu pokazali puno interesovanja za upotrebu ove vrste kartica.

6.6.6. Digitalni čekovni platni sistemi

Čekovi postaju sve više negotovinski način plaćanja: 2000. godine je u SAD-u ispisano 65 milijardi čekova, a broj raste sa stopom od oko 1 milijardu godišnje – tri puta više od porasta kreditnih kartica, debitnih kartica i drugih vrsta elektronskog transfera novca. Nažalost, procesiranje čeka košta između 0.75 i 3.00 dolara. Centralna banka SAD-a procenjuje da to košta američku ekonomiju 44 milijarde dolara godišnje. Čekovi su spor način plaćanja i oni zahtevaju koverat i poštansku markicu. Digitalni čekovni platni sistem nudi drugačije rešenje.

Digitalni čekovni platni sistemi pokušavaju da prošire delatnost postojećih čekovnih računa na onlajn kupovine. Stoga se mogu posmatrati i kao proširenje postojeće čekovne i bankovne infrastrukture. Neki od jednostavnijih sistema koriste se da elektronskim putem plaćaju fizičkim licima i da naprave račune na sajtovima za aukcije. Sofisticiranije sisteme koristi Treasury Department da elektronskim putem prenosi velike dolarske iznose. Digitalni čekovni platni sistemi imaju više prednosti: (1) kupci ne moraju da odaju svoje podatke drugim licima, (2) kupci ne moraju konstantno da daju svoje podatke na Web-u, (3) prodavcima su jeftiniji od kreditnih kartica, i (4) mnogo su brži od uobičajenih papirnih čekova. Tabela 6.6.6. pokazuje neke od najpoznatijih digitalnih čekovnih sistema.

Jedan od najjednostavnijih digitalnih čekovnih sistema je Achex. Achex je primarno napravljen kao mali P2P platni mehanizam za transfer novca između pojedinaca. Korisnik otvori na sajtu Achex-a račun i daje broj svog čekovnog računa koji će koristiti prilikom plaćanja. Kada se račun proveri, korisnici Achex-a mogu da plaćaju drugim osobama koje imaju e-mail adresu i validni čekovni račun na koji može da se prenese novac. Korisnik ulazi u Achex račun preko svog korisničkog imena i lozinke ili PIN-a. Primalac dobije e-mail u kome mu je saopšteno da ima raspoloživih redstava za transfer i

u kome se traži validni broj čekovnog računa na koji će novac biti prenesen. Achex, zatim, izvrsi transfer novca na čekovni račun primaoca. Ova usluga je besplatna za kupce, dok prodavci plaćaju taksu za ceo proces, koja je upola niža od taksi za kreditne kartice.

Tabela 6.6.6 Digitalni čekovni platni sistemi

SISTEM	GODINJA OSNIVANJA/OPIS
eCheck	1998. Konzorcijum od 15 banaka, vladinih agencija i tehnoloških kompanija (Echeck.org). Bezbedan elektronski čekovni sistem. Potreban digitalni novčanik.
Achex Inc.	1999. Jednostavan čekovni sistem. Nije potreban digitalni novčanik.
BillPoint Electronic Checks	2000. eBay, Wells Fargo su ušli u onlajn digitalni sistem čekova, ali samo za upotrebu u okviru eBay-a. Nije potreban digitalni novčanik.

eCheck je sofisticiraniji sistem. Konzorcijum banaka, vladinih agencija i tehnoloških kompanija su 1995. godine počele da razvijaju projekat za elektronsko plaćanje čekovima u kojem bi bilo korišćeno šifrovanje javnim ključem i za koji ne bilo potrebno treće lice (kao Achex), kako bi se sredstva prenela. Cilj je bio da se ovim sistemom zamene papirni čekovi i da se prošire elektronski transferi novca, koji već postoje u okviru velikih institucija, na sve prodavce uključujući i kupce. Slika 6.6.7. pokazuje kako funkcioniše eCheck.

Sl. 6.6.7. Kako funkcioniše digitalni čekovi eCheck

Kao što se vidi na slici 6.6.7., eChecks zahteva od korisnika da od tradicionalne banke dobije "elektronski čekovnik" baziran na hardveru. Hardver može biti PCMCIA kartica, standardna PC kartica ili specijalni eksterni čitač za smart karticu. Elektronski čekovnik sadrži digitalni potpis korisnika u obliku privatnog ključa. Elektronski čekovnik takođe sadrži javni ključ banke koja ga je izdala (#1). Preko softvera koji se dobija uz elektronski čekovnik, kupac popunjava elektronski ček i šalje ga prodavcu preko Interneta (#2). Komunikacija je šifrovana i sadrži digitalni potpis kupca, javni ključ i digitalni potpis matične banke. Prodavac zatim identifikuje digitalne potpise obe strane, koristeći njihove javne ključeve (#3A, #3B), i deponuje čekove u svoju banku (#4). Viši stepen autoriteta za čekove, kao što je Centralna banka, potvrđuje javni ključ banke koja je izdala čekove (#5). eChecks mogu takođe da sadrže i podatke o robi, podatke o sumi robe koja je poslata i druge informacije.

eCheck je interesantan zbog toga što je elektronski čekovnik fizičko sredstvo, koje je sigurnije od računa na Internetu. Iako je bilo zamišljeno da se integriše u postojeću infrastrukturu čekovnog sistema, ipak eCheck zahteva značajna ulaganja u novu infrastruktruru.

6.6.7. Digitalni platni sistemi i bezični Internet

Bežični uređaji su doživeli svoj procvat i očekuje se da će se taj eksplozivni trend razvoja nastaviti. Od mobilnih telefona do pejdžera i personalnih digitalnih asistenata (PDA), bežični uređaji su podstakli stvaranje novih Web sajtova koji ih podržavaju. Oblast gde postoji dosta interesovanja su finasijske usluge, uključujući, berzansko trgovanje i transfer novca. Korišćenje mobilnog telefona kao sistema za plaćanje je naročiti razvijeno u Evropi, Japanu i Južnoj koreji. Japanci već uveliko koriste sisteme plaćanja preko mobilnog telefona zasnovane na e-gotovini, mobilnim debitnim i kreditnim karticama. Procenjuje se da će rast Wi-Fi-ja i 3G mobilne telefonije ove sisteme učiniti globalnim i sveprisutnim.

6.7 B2B PLATNI SISTEMI

Većina platnih sistema o kojima je bilo reči se prvenstveno koriste u B2C trgovini. B2B platni sistemi postavljaju mnoge izazove i daleko su kompleksniji od B2C plaćanja, uglavnom zbog kompleksnosti poslovnih transakcija. Ponekad je potreban veliki broj dokumenata da bi se obavila transakcija, uključujući narudžbenicu, podatke o robi, račun, isporuku, papire o osiguranju, finansijske dokumente, zakonske dokumente, verifikacije kredita, usluge treće strane (ako ima), identifikaciju, pisma o kreditu (strane transakcije), i platni metodi i instrumenti. B2B sistem mora da se poveže sa postojećim ERP (Enterprise Resource Planning) sistemima koji integrišu podatke o inventaru, proizvodnji,

isporuci i druge korporativne podatke, i sa EDI (Electronic Data Interchange) sistemima, koji zamenjuju narudžbine na papiru, elektronskom formom narudžbenica. Tabela 6.7.1. opisuje neke od karakteristika B2B platnih sistema.

B2B platno tržište je trenutno mnogo veće od B2C tržišta, zbog većeg broja transakcija između poslovnih subjekata. U SAD-u se većina plaćanja između kompanija odvija fizičkim čekovima koji prolaze kroz Automated Clearing House (ACH) platni sistem koji vrši Centralna banka. U rastućem broju transakcija, to se odigrava preko elektronskog transfera sredstava. U Evropi su fizički čekovi manje zastupljeni, a u nekim zemljama, kao što je Holandija, skoro sva poslovna plaćanja se vrše elektronskim putem kroz razvijenije bankarske sisteme.

Postoje dva velika tipa B2B platnih sistema: sistemi koji zamenjuju tradicionalne banke i sistemi koji postojeće bankarske sisteme prilagođavaju B2B tržištu. Pri tome, važno je napomenuti da nijedan današnji sistem nema sve opcije koje se nalaze u prikazanoj tabeli 6.7.1.

Actrade je jedan primer onlajn B2B platnog sistema, koji zamenjuje funkcije koje pružaju tradicionalne banke. Actrade radi kao međunarodni posrednik na tržištu platnih procesa, tako što strane prodavce isplaćuje odmah, a domaćim kupcima nudi određeni vremenski period za plaćanje. Actrade rešava prodavcima rizik oko kredita jer ih odmah isplaćuje. Transakcije su potpuno digitalne i bezbedne i imaju digitalne sertifikate. Druge konkurentske firme u B2B platnom sistemu uključuju TradeCard, eRevenue, eFinance i Echeck za male poslovne transakcije.

Dok su tradicionalne banke bile spore pri ulasku na tržište, one sada nude široku lepezu usluga onlajn. Orbian je nastao od udruživanja Citigroup-a i SAP-a, nemačkog softverskog giganta. Orbian nudi finansijske kredite slično kao Actrade, ali podrazumeva i verifikaciju kredita, neodbijanje plaćanja, finansiranje i integraciju u velike firme back-end sistema. Drugi gigant je FinancialSettlementMatrix.com (FSM), koga čine velike banke kao što su WellsFargo i Citibank, u zajednici sa tehnološkim kompanijama kao što su i2 Technologies i S1. FSM je jedini platni sistem koji može da radi sa nekoliko banaka i nudi kreditna pisma, posredstvo trećeg lica, međunarodne transfere, finansiranje i kreditne čekove. Za manje transakcije, tradicionalne kompanije kreditnih kartica kao MasterCard i AmericanExpress su razvile "P-cards", odnosno prenosne kartice. Trenutno ograničene na transakcije manje od 2,500 dolara, neke kreditne kompanije razmišljaju o transakcijama P-karticom do 100,000 dolara. P-kartice nemaju narudžbenice ili praćenje dokumentacije o robi i zato se ne koriste za veće transakcije.

Tabela 6.7.1 Ključne karakteristike B2B platnih sistema

KARAKTERISTIKA	OPIS
Verifikacija kredita i garancija	Daje evaluaciju kredita i platnu garanciju
Servis zaloga	Osigurava da obe strane ispune svoje obaveze
Neporecivost	Osigurava da plaćanje kupljenog ne bude odbijeno; omogućava stranama koje se ne poznaju da bezbedno trguju
Sakupljanje sredstava za prodavca	Radi transfer sredstava i čuvanje
Finansiranje	Obezbeđuje "float" ili odlaganje plaćanja prodavcima koji za to dobijaju prihod od takse
Integracija sa drugim poslovnim dokumentima	Integriše narudžbine, podatke o robi, slanje dokumenata i plaćanje
Detekcija prevara	Pomaže prodavcima da bezbednije trguju
Računovodstvo	Prikaz sadrzaja računa i odgovarjućih detalja
Rešavanje sporova	Omogućava metodu za rešavanje sporova
Integracija sa korporativnim sistemima za podršku	Povezuje platne sisteme sa transportom, računovodstvom i drugim korporativnim sistemima
Onlajn računi	Ima sposobnost da pravi i prezentuje elektronske račune
Mnogobrojne opcije plaćanja	Omogućava kupcima da plaćaju kreditnim karticama, debitnim karticama, ACH čekovima, elektronskim transferom novca i dr.

6.7.1. Elektronsko prezentovanje i plaćanje računa

Procena je da se u USA mesečno generiše oko 30 milijardi računa koje plaća oko 200 miliona potrošača i nekoliko miliona kompanija. Neki stručnjaci smatraju da se cena životnog ciklusa računa, od izdavanja do plaćanja, kreće od $3 do $7. Ovaj račun ne obuhvata vreme koje potrošaci koriste da bi otvorili račune, pročitali ih, napisali čekove, adresirali koverte, zalepili poštansku markicu i najzad ih poslali. Ne računajući troškove potrošača, ukupni troškovi za račune se kreću od 360 do 840 milijardi dolara, ili od 4% do 8% od BNP-a. Tržište računa čini izuzetnu priliku za upotrebu Internet tehnologije u cilju smanjenja troškova plaćanja računa i vremena koje se tom prilikom troši. Kako su potrošači sve više onlajn, logično je očekivati da će koristiti Internet kao sredstvo za efikasno plaćanje računa.

Elektronski sistemi prezentovanja i plaćanja ili EBPP, su novi vidovi onlajn platnih sistema za mesečne račune. Potrošači mogu pomoću EBPP-a da vide svoje račune elektronskim putem i da ih plaćaju preko elektronskog transfera sredstava od banke

ili računa kreditnih kartica. Sve više kompanija bira izdavanje računa elektronskim putem, izbegavajući slanje regularnom poštom. Čak i one firme koje šalju račune regularnom poštom, sve više nude opciju slanja računa elektronskim putem, što dozvoljava potrošačima da odmah izvrše transfer sredstava sa bankovnog računa kako bi platili račun bilo gde u svetu. Procenjuje sa da danas u SAD 50% domaćinstava već koriste neki od EBPP sistema. Očekivani rast je čitavih 75% do 2012. godine.

Iako se preko 90% svih EBPP-a dešava u B2C sektoru, ti platni sistemi se brzo šire na B2B trgovinu. Izazovi vezani za plaćanje računa elektronskim puten su isti i za potrošače i za preduzeća, osim što su poslovne transakcije po pravilu sa mnogo većim iznosima novca. Iako početni kapital za implementaciju EBPP sistema može da iznosi $100,000, taj novac se brzo isplati. Jedna kompanija, North Pittsburgh Telephone, procenjuje da će uštedeti 80% posle uvođenja sistema elektronske prezentacije i naplate računa.

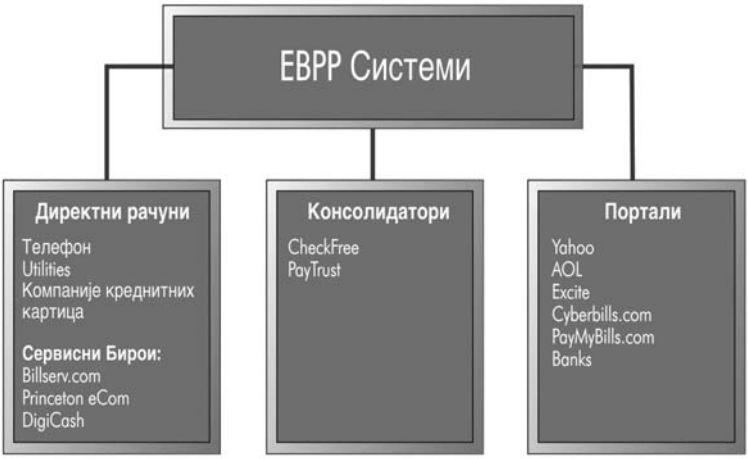
6.7.2. Vrste EBPP sistema

Iako je koncept onlajn prezentacije i plaćanja računa jednostavan, postoji veliki broj konkurentnih poslovnih modela na tržištu. Najuobičajeniji je sistem direktnog računa, koga su osmislile velike kompanije koje šalju svakog meseca milione računa. Cilj je da njihovi klijenti na što lakši način plate svoje mesečne i druge račune onlajn. Telefonske kompanije, kompanije kreditnih kartica, kao i individualne prodavnice često nude ovu uslugu. Po pravilu ovi sistemi koriste servisni biro, kao što je BillServ.com, kako bi obezbedili neophodnu infrastrukturu za implementaciju sistema. Druga velika vrsta EBPP-a je konsolidatorski model. Konsolidatori sakupljaju sve račune svojih klijenata i omogućavaju one-stop plaćanje računa. Portali su slični konsolidatorima, i nude skup drugih usluga finansijskog menadžmenta. Slika 6.7.1. ilustruje glavne tipove EBPP sistema.

Kompanije mogu koristiti EBPP samo da ispostave račune potrošačima na elektronski način ili da ugovore kompletanu uslugu naplate računa. Potrošači onda mogu da izaberu da direktno plate račun, da koriste konsolidatorski račun koji sakuplja račune za njih ili da unajme platnu uslugu da sakuplja i plaća račune, na način kako potrošač odredi. BlueGill Technologies je kompanija direktne naplate, koja omogućava potrošačima da posete Web sajt na kome mogu da pogledaju svoje račune i da ih plate. CheckFree je konsolidator koji sakuplja i izdaje račune sa mnogobrojnih izvora, tako da potrošač treba samo da se uloguje na sajt, kako bi odednom platio nekoliko računa. CyberBills funkcioniše slično kao CheckFree, ali se razlikuje u tome što izveštaj šalje od naplatnika do servisa, a ne direktno potrošaču. MessagingDirect šalje izveštaje i račune e-mail-om direktnim linkom prodavcu na Web sajt radi lakšeg plaćanja.

U proces naplate su uključeni potrošač, banka i potencijalno treća strana. Potrošač može da pošalje e-mail-om e-ček na bankovni račun i sredstva se prenose e-mail-om na račun potražioca.

U konkurenciji na EBPP tržištu, neke kompanije vode. Web portali, kompanije raznih potrebština i tradicionalne banke već imaju deo infrastrukture koja je potrebna za izgradnju efikasnog EBPP sistema. Najjači igrači su Web portali kao na primer AOL i Yahoo. Udruživanjem sa firmama koje imaju softver, kao na pr. CheckFree i tradicionalne banke, oni su u mogućnosti da ponude potrošačima plaćanje računa kao deo paketa usluga finansijskog menadžmenta.



Sl. 6.7.1. Vrste EBPP sistema

6.8 LITERATURA

[1] https://www.paypal.com/

[2] http://en.wikipedia.org/wiki/PayPal

[3] MacKie-Mason, K. Jeffrey, K. White, " Evaluating and Selecting Digital Payement Mechanisms", *Telecommunications Policy Research Conference*, Maryland, 1996.

[4] http://www.gartner.com/technology/home.jsp

[5] K.Laudon, C.Traver, E-Commerce: Business, Technology, 6.th ed., Boston, Addison-Wesley, 2009.

[6] http://www.kosmix.com/topic/digital_wallet

[7] http://www.mastercard.com/index.html

[8] http://en.wikipedia.org/wiki/Windows_Live_ID

[9] IETF Network Working Group," Electronic Commerce Modeling Language (ECML) Version 2 Specification", http://www.ietf.org/rfc/rfc4112.txt

[10] Qpass, Inc., "Qpass Provides Back Office Support for AT&T Wireless GoPort Service", 2003.

[11] S. Glassman, M. Manasse, M. Abadi, P. Gauthier, P. Sobalvarro, "The Millicent Protocol for Inexpensive Electronic Commerce", *In Proceedings of Fourth International World Wide Web Conference,* Boston, USA, 1995. http://www.w3.org/Conferences/WWW4/Papers/246/

7. MARKETING U ELEKTRONSKOJ TRGOVINI

U ovom poglavlju se ukratko izlažu osnovni koncepti marketinga i njihova primena u elektronskoj trgovini, tehnologije Internet marketinga i strategije marketinga i brendiranja u elektronskoj trgovini.

Poznavanje osnova marketinga neophodno je za razvoj elektronske trgovine i uspešno poslovanje na Internetu.

Marketing čine strategije i aktivnosti firme, koje se preduzimaju radi uspostavljanja odnosa sa potrošačem i podsticanja kupovina svojih proizvoda ili usluga [1].

Specifičnost Internet marketinga je upotreba Web-a, uz tradicionalne prodajne kanale, za razvoj pozitivnih, dugoročnih odnosa sa *online* i *offline* kupcima i time stvaranje konkurentske prednosti za firmu, koja omogućava postizanje viših cena proizvoda ili usluga nego što može da ostvari konkurencija.

7.1. INTERNET KORISNICI I PONAŠANJE POTROŠAČA NA INTERNETU

Osnovni princip marketinga i prodaje je poznavanje potrošača, u ovom slučaju Internet korisnika. Neki osnovni statistički podaci o Internet korisnicima, za područje SAD, mogu se pronaći u [1],[2], [3]: kakva je struktura korisnika Interneta, odnosno ko, kako i šta kupuje na Internetu.

Pristup Internetu je 2009. godine u SAD imalo više od 72% domaćinstava, dok 98% poseduje TV, a 94% telefon. Dugogodišnja visoka stopa rasta broja Internet korisnika je usporena, ali se zato povećava intenzitet i obim korišćenja. Raspodela korišćenja nije ravnomerna po osnovnim demografskim karakteristikama (polu, uzrastu, etničkoj pripadnosti, društvenom tipu, prihodima i obrazovanju).

Prema podacima Republičkog zavoda za statistiku za 2010 [4], u Srbiji Internet priključak poseduje 39% domaćinstava, 98,7% poseduje TV, 82% mobilni telefon, a 50,4% poseduje računar.

U SAD, prema načinu pristupa Internetu, 82% Internet korisnika koristi širokopojasni pristup. Od ukupnog broja domaćinstava u Srbiji koja poseduju Internet priključak, širokopojasni DSL (ADSL) pristup ima 47,3% domaćinstava, kablovski Internet 24,5%, WAP i GPRS 20% domaćinstava, a modemsku konekciju 17,5%.

Istraživanje je pokazalo da *širokopojasni pristup* Internetu koriste bogatiji, sredovečni i obrazovaniji korisnici.

Ponašanje okoline znatno utiče na ponašanje u kupovini. Pokazalo se da život u blizini onih koji kupuju u *online* prodavnicama prehrambenih namirnica povećava verovatnoću kupovine za 50%.

Intenzitet korišćenja Interneta zavisi od *stila života i društvenih uticaja*. Deca i tinejdžeri koriste Internet kao zamenu za neke društvene aktivnosti, kao što je međusobno druženje i kontakti sa susedima i članovima porodice. Radno aktivni takođe manje vremena provode s porodicom i prijateljima, a više u radu, na poslu ili kod kuće. S druge strane, razvile su se sasvim nove društvene aktivnosti vezane za upotrebu Interneta.

Stručnjaci za marketing posebno prate konkuretski odnos Interneta i tradicionalnih medija, kao što su štampa, televizija i radio. Istraživanja pokazuju da je sadašnja upotreba Interneta dovela do smanjenja interesovanja za televiziju u važnim demografskim grupama, kao što su mladi ljudi i zdravi i obrazovani, za 25-30%.

7.1.1 Modeli ponašanja potrošača

Proučavanje ponašanja potrošača je disciplina društvenih nauka, koja nastoji da modelira i shvati ponašanje ljudi na tržištu [1]. Modeliranje ponašanja potrošača pokušava da predvidi šta će potrošači kupiti i gde, kada i koliko da objasni zašto kupuju.

Modeli ponašanja potrošača predviđaju širok spektar potrošačkih odluka, koje se zasnivaju na nezavisnim demografskim faktorima i skupu posredujućih (intervenišućih) faktora, koji neposrednije oblikuju odluke potrošača.

Opšti model ponašanja potrošača, Slika 7.1, zasniva se na:

- demografskim faktorima kao nezavisnim promenljivima;
- intervenišućim promenljivima, koje stimuliše tržište i
- zavisnim promenljivima, odlukama kupaca.

Demografski faktori mogu biti kulturne, društvene ili psihološke prirode. *Kultura* je najopštiji faktor ponašanja potrošača, jer oblikuje osnovne ljudske vrednosti, želje, percepciju i ponašanje. Kultura kreira osnovna očekivanja potrošača, kao što je šta i kako treba kupovati na nekom tržištu, što je veoma značajno za internacionalni marketing.

Npr. e-prodaja prehrambenih artikala uobičajena u Americi, dok u Kini i Japanu velike prodavnice hrane ne postoje, već se hrana kupuje u lokalnim prodavnicama u susedstvu, gde se pre odluke o kupovini proba ukus i miris hrane.

Slika 7.1 Opšti model ponašanja potrošača

Unutar velikih nacionalnih kultura, ponašanje potrošača veoma zavisi od pripadnosti subkulturnim grupama, koje se formiraju prema raznim društvenim različitostima, kao što su entnička pripadnost, starosno doba, stil života i geografski položaj. Subkulturne grupe se mogu posmatrati kao zasebni segmenti tržišta.

Važni *društveni* demografski faktori koji oblikuju ponašanje potrošača su referentne grupe, kojima potrošači pripadaju direktno ili indirektno, preko srodstva, udruživanja ili sklonosti. *Direktne* referentne grupe uključuju porodicu, profesiju, religiju, susedstvo ili školu, a *indirektne* neku fazu života, društveni sloj i životni stil. Npr. društvene mreže okupljaju članove sa sličnim interesovanjima, kao što su pripadnici školske generacije ili rekreativnih aktivnosti.

U svim referentnim interesnim grupama postoje predvodnici javnog mnenja (*viral influencers*), koji utiču na ponašanje drugih svojom ličnošću, sposobnostima ili drugim faktorima.

Jedna od referentnih grupa se formira na osnovu *stila života* (*lifestyle*), odnosno obrazaca aktivnosti (sport, hobiji, kupovanje, prisustvo određenim skupovima), interesovanja (hrana, moda, rekreacija) i opredeljenja (društvena pitanja, poslovanje, država). Poznavanje stila života pomaže u dizajnu specifičnih proizvoda i marketinga za tu grupu, odnosno segmentaciji tržišta.

Psihološki profil je skup potreba, podsticajnih faktora, motivacija, percepcija i naučenog ponašanja, uključujući stavove i ubeđenja. Stručnjaci marketinga koriste psihološke profile prilikom dizajniranja i pozicioniranja proizvoda i za marketinške komunikacije.

Pošto osnovni demografski faktori ne daju dovoljno detaljnu sliku tipičnog potrošača u elektronskoj trgovini, kombinuju se demografski i psihološki podaci radi kreiranja demografsko-psihološkog (*psychographic*) profila, kojim se tržište deli na osnovu socijalnog sloja, životnog stila i ličnih karakteristika.

Istraživanja pokazuju da su najznačajniji faktori za predviđanje ponašanja potrošača prilikom kupovine (1) traženje informacija o prozvodima *online* (2) značajan deo radnog i privatnog života *online,* npr. broj poruka e-pošte i (3) nedavno izvršene narudžbe putem *online* kataloga.

Proces donošenja odluke o kupovini na mreži može se podeliti u pet faza [1]:

- svest o potrebi
- traganje za više informacija
- procena alternativa
- konkretna odluka o kupovini
- kontakt sa firmom nakon kupovine

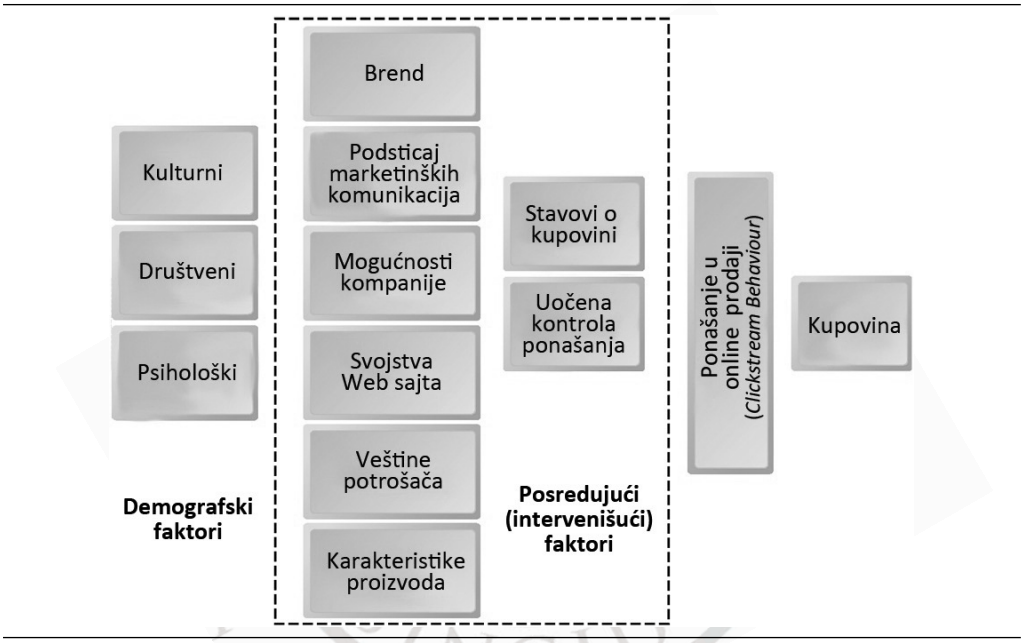
Na Slici 7.2 prikazan je proces donošenja odluke o kupovini i podrška različitih oblika *online* i *offline* marketinških komunikacija svakoj od faza. Specifičnost *online* kupovine je dopuna klasičnuh marketinškuh komunikacija mogućnostima koje pruža Web, kao što su npr. razmena poruka, ekranske reklame (baneri), ciljane poruke e-pošte, pretraživači i *online* prikazi proizvoda.

MARKETINŠKE KOMUNIKACIJE	Svest o potrebi	Traganje za informacijama	Procena alternativa	Kupovina	Kontakt nakon kupovine
offline	• masovni mediji • TV, radio • štampa	• katalozi • štampane reklame • masovni mediji • prodavci • ocenjivači proizvoda • posete	• referentne grupe • predvodnici javnog mnjenja • masovni mediji • ocenjivači proizvoda • posete	• promocije • direktna pošta • masovni mediji • štampa	• garancija • servis • delovi i opravke • korisničke grupe
online	• ciljane baner reklame • iskačuće/ zaklonjene Web reklame • ciljane promocije	• pretraživači • online katalozi • posete sajtu • prikazi proizvoda • ocene korisnika	• pretraživači • online katalozi • posete sajtu • prikazi proizvoda • ocene korisnika	• online promocije • lutrije • popusti • ciljana e-pošta	• udruženja korisnika • bilteni • korisnička e-pošta • online update

Slika 7.2 Proces donošenja odluke o online kupovini i marketinške komunikacija

7.1.2 Model ponašanja potrošača na mreži

Ponašanje potrošača na mreži ima mnogo zajedničkog sa opštim modelom ponašanja potrošača, ali i neke specifičnosti. Opšti model treba dopuniti novim faktorima, pre svega osobinama korisnika, svojstvima proizvoda i mogućnostima Web sajta, dok je ponašanje potrošača u prodavnici zamenjeno ponašanjem potrošača prilikom *online* kupovine (*clickstream behaviour*), Slika 7.3.



Slika 7.3 Model ponašanja potrošača na mreži (*online*)

Mogućnosti Web sajta su njegov sadržaj, dizajn i funkcionalnost, koja se ogleda u brzini odziva, mogućnosti navigacije i poverenju u bezbednost podataka. Veštine potrošača se odnose na poznavanje procesa vršenja online transakcija. Karaktersistike proizvoda utiču tako što je neke od proizvoda lakše opisati, spakovati i poslati preko Interneta, kao npr. digitalne sadržaje poput knjiga, softvera, DVD izdanja.

Stavovi o kupovini se odnose na poverenje u Web sajt i pozitivno ranije iskustvo u Web kupovini. Uočena kontrola ponašanja je osećaj korisnika da kontroliše svoje okruženje na Web sajtu.

Poznavanje ponašanja u *online* prodaji (*clickstream behaviour*) ima istu ulogu kao i poznavanje ponašanja potrošača u prodavnici prilikom klasične kupovine – pomaže da se skrati put do proizvoda koji se najčešće traže. Podaci o akcijama, odnosno ponašanju potrošača, pamte se u dnevniku transakcija.

Tipični obrasci ponašanja prilikom *online* kupovine dati su u Tabeli 7.1 u obliku tipičnih korisničkih sesija.

Tabela 7.1 Tipovi online sesija

	***Online* ponašanje**	**Trajanje sesije (min)**	**Trajanje po stranici (min)**	**Familijar-rnost**	**Koncen-tracija**
1.	*Quickies* - traže sport, čitaju e-poštu	1	0,25	90%	90%
2.	*Just the Facts* - pronalaze i ocenjuju informacije sa srodnih sajtova	9	0,5	88%	47%
3.	*Single Mission* - odlaze na nepoznate sajtove iste kategorije da pronađu traženo	10	1,5	11%	85%
4.	*Do It Again* - odlaze na omiljene sajtove, npr.. bankarstvo i chat sobe	14	2	95%	87%
5.	*Loitering* - leženo obilaze omiljene sajtove, vesti i igre	33	2	90%	87%
6.	*Information Please* - istražuju sve aspekte teme sa više sajtova	37	1	14%	41 %
7.	*Surfing* - usmeren na istraživanje, na sajtove kao što su vesti i kupovina	70	1	14%	26%

Prema [1], preko 86% Internet korisnika kupuje online, tražeći ili kupujući proizvode. Posmatrači su oni koji traže i biraju proizvode *online*, a kupuju *offline*, svega 16% korisnika, dok 64% korisnika kupuje *online*, Slika 7.4.

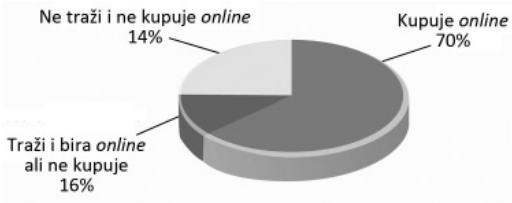
Jedna trećina klasične *offline* kupovine na malo vrši se na osnovu informacija i pod uticajem aktivnosti na mreži. Istovremeno je *online* saobraćaj pod uticajem *offline* robne marke, odnosno kupovine.

Elektronska trgovina i tradicionalne trgovine su u sprezi i predstavljaju delove kontinuuma potriošačkog ponašanja.

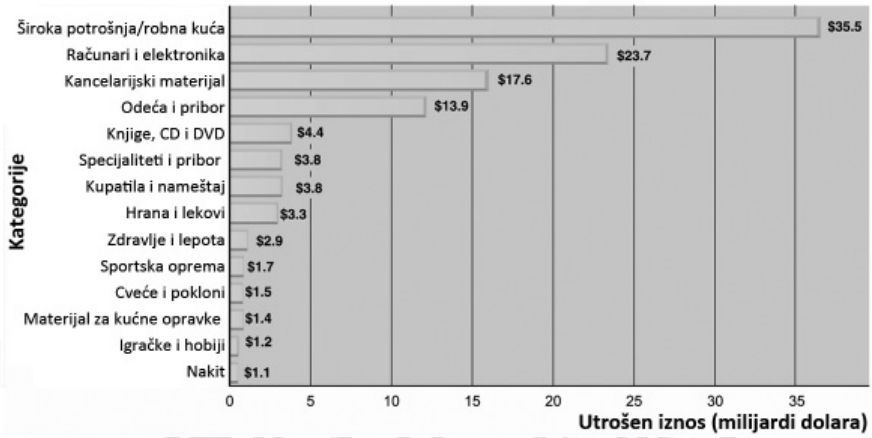
Online prodaja se deli grubo na stavke malih vrednosti i stavke velikih vrednosti. Stavke malih vrednosti (do 100$) tradicionalno uključuju aparate, knjige, lekove i kozmetiku, kancelarijski materijal, muziku, softver, video sadržaje, igračke itd.

Glavne kategorije stavki malih vrednosti imaju slične karakteristike - prodaju ih prvi pokretači na *online* tržištu, cene su niske, fizički su mali, marža je visoka, a izbor raspoloživih proizvoda velik.

Stavke velikih vrednosti (preko 500$) su npr. avionske karte, hotelske sobe, računarski hardver, potrošna elektronika itd. i sve se više kupuju *online*.



Slika 7.4 Online posmatrači i kupci (Shoppers and Buyers)



Slika 7.5 Šta potrošači kupuju online

Velika većina kupaca do sajta e-trgovine dolazi direktnim unosom Web adrese ili pomoću pretraživača, tražeći određeni proizvod ili proizvođača. Online kupci su usmereni na određene proizvode, kompanije i usluge i pri tome [1]:

- 37% kupaca koristi pretraživače;
- 33% direktno pristupa Web sajtu e-trgovine;
- 17% koristi komparaciju na Web sajtovima za kupovinu;
- 15% koristi Web sajtove sa rangiranjem proizvoda.

Neki od razloga zbog kojih veći broj potrošača ne kupuje *online* su:

- 44% oseća nelagodnost zbog *online* upotrebe kreditne kartice;
- 42% je zabrinuto za zaštitu privatnosti podataka;
- 37% ne voli troškove dostave proizvoda kupljenih *online*;
- 33% smatra da nema potrebe za kupovinu na mreži;
- 32% više voli da dodiruje/oseti proizvod pre kupovine;
- 27% nalazi da je vraćanje proizvoda usled reklamacije suviše teško;
- 21% nije našlo na mreži ništa zanimljivo za kupovinu.

Istraživanja pokazuju da su najvažniji faktori koji oblikuju odluku o online kupovini korisnost (*utility*) i poverenje (*trust*). Potrošači su uvek u potrazi za boljom cenom, većom udobnosti kupovine i brzinom isporuke, odnosno traže korisnost.

Informaciona asimetrija može dovesti do oportunističkog ponašanja prodavaca, koji mnogo više znaju o proizvodu i uslovima prodaje. Zato potrošači moraju da veruju trgovcu pre nego što budu spremni na kupovinu. Prodavci moraju da razviju poverenje kupaca tako što stvaraju reputaciju iskrenosti, poštenja i isporuke kvalitetnih proizvoda, što su osnovni elementi brenda. Za to se koriste forumi i drugi oblici prikupljanja i objavljivanja povratnih informacija. Prodavci koji razviju poverenje potrošača mogu da postignu više cene proizvoda i usluga na tržištu.

7.2 OSNOVNI KONCEPTI MARKETINGA

Marketing obuhvata strategije i akcije firmi preduzete da se uspostavi odnos sa potrošačem i ohrabri kupovina proizvoda i usluga [1].

Internet marketing se odnosi na korišćenje Web-a, kao i tradicionalnih kanala, radi razvijanja pozitivnog dugoročnog odnosa sa potrošačima, čime se stvara komparativna prednost za firmu, što omogućava postizanje veće cene proizvoda i usluga u odnosu na konkurente [1].

Industrijske firme međusobno konkurišu u četiri dimenzije:

- diferencijacija (različitost)
- troškovi
- obim
- fokus

Marketing se neposredno bavi konkurencijom firmi i teži kreiranju jedinstvenih, veoma različitih (diferenciranih) proizvoda ili usluga, koje proizvodi ili pruža jedna pouzdana firma. Monopolski položaj firme smanjuje pregovaračku snagu potrošača, jer predstavlja jedinog dobavljača. Marketing se koristi i za sprečavanje da proizvod postane *roba*. Roba su dobra ili usluge za koje postoji veliki broj prodavaca i svi proizvodi suštinski identični, npr. pšenica ili čelik. Izbor kupca se zasniva isključivo na ceni i uslovima isporuke.

Marketing nastoji da izbegne isključivo konkurenciju cena i da kreira tržište gde je povrat investicija prosečan, konkurencija ograničena i gde će kupci plaćati više cene proizvoda, koje doživljavaju kao jedinstvene.

Marketinški ciljevi su:

- Izbegavati čistu konkurenciju cenama, jer tako proizvodi postaju roba
- Ograničenje konkurencije, zamena proizvoda
- Povećanje diferencijacija proizvoda
- Naglasiti ostale kvaliteta proizvoda

7.2.1 Skupovi karakteristika

Osnovni zadatak marketinga je identifikacija i saopštavanje kupcu jedinstvenih, diferenciranih mogućnosti i usluga *skupova karakteristika* proizvoda ili usluge. Skupovi karakteristika (*feature sets*) definišu se kao skup *svojstava* i *usluga* koje proizvodi i servisi nude.

Skupovi karakteristika uključuju, Slika 7.6:

- osnovnu vrednost proizvoda (*core product*), odnosno ključnu dobit koju kupac dobija od proizvoda, npr. mobilni telefon;
- aktuelnu vrednost proizvoda, koja obuhvata skup karakteristika dizajniranih da se isporuči glavna vrednost proizvoda, npr. mobilni telefon sa muzičkim plejerom i velikim ekranom, koji se preko bežične mreže povezuje na Internet;
- povećanu vrednost proizvoda, dodatnu korist, benefit za kupce koje proizvod daje izvan glavne vrednosti ugrađene u aktuelni proizvod, npr. garancija i korisnička podrška.

Slika 7.6 Skup karakteristika proizvoda

7.2.2 Brendovi i brendiranje

Brend predstavlja skup očekivanja koja kupci imaju kada kupuju ili misle da kupuju neki proizvod ili servis od specifične kompanije. Najvažnija očekivanja su: kvalitet (*quality*), pouzdanost (*reliability*), trajnost (*consistency*), poverenje (*trust*), privrženost (*affection*), odanost (*loyalty*) i renome (*reputation*). *Brendiranje* je proces stvaranja brenda.

Zatvorena petlja marketinga je situacija kada agenti marketinga mogu drektno da utiču na dizajn osnovne vrednosti (*core*) proizvoda na bazi istraživanja tržišta i povratne informacije. Elektronska trgovina povećava mogućnost dostizanja zatvorene petlje marketinga.

Strategija brendiranja je skup planova za diferencijaciju proizvoda od konkurenata i komunikaciju ovih razlika na prostor za trgovinu.

Vrednost brenda (*brand equity*) je procenjena vrednost premije koju je kupac voljan da plati za brendirani proizvod u odnosu na nebrendirane proizvode konkurenata.

Na Slici 7.7 prikazan je proces brendiranja, odnosno aktivnosti marketinga od kreiranja proizvoda do brenda.

Slika 7.7 Proces kreiranja brenda

7.2.3 Segmentacija, ciljanje i pozicioniranje

Tržište se sastoji od velikog broja različitih vrsta potrošača sa različitim potrebama. Kompanije teže da *segmentiraju* tržište na grupe potrošača sa različitim potrebama za proizvodima, nakon čega se grupe *ciljaju* diferenciranim proizvodima. Unutar svakog segmenta proizvod se *pozicionira* i brendira kao jedinsven, visoko cenjem proizvod, posebno pogodan za potrošače posmatranog segmenta.

Glavni vrste segmentiranja i ciljanja potrošača su:

- prema ponašanju
- demografski
- psihografski
- tehnički
- kontekstualni
- pretraživanje

Jedno od važnih pitanja je da li su brendovi racionalni. Iz perspektive potrošača, odgovor je *najverovatnije potvrdan*, jer brendovi povećavaju efikasnost tržišta smanjenjem aktivnosti pretraživanja i troškova donošenja odluka o kupovini.

Za poslovne subjekte, odgovor je *definitivno potvrdan*, jer brendovi (1) smanjuju troškove pronalaženja kupaca, odnosno ukupne troškove konverzije perspektive prodaje u potrošnju i (2) povećavaju vreme zadržavanja kupaca. Uspešan brend sadrži dugotrajnu (mada ne neophodno permanentnu) nefer konkurentsku prednost.

Takođe je važno pitanje da li će brendovi opstati na Internetu. Istraživači inicijalno pretpostavljaju da bi Web mogao rezultirati u "zakonu jedne cene", jer bi sa potpunom transparentnošću i perfektnim tržištem, postojala samo jedinstvena svetska cena za svaki proizvod. Ako se to ne dogodi, e-trgovinske firme će nastaviti da se oslanjanju na brendove radi privlačenja kupaca i naplate premijerne cene.

Disperzija cena je razlika najviših i najnižih cena na tržištu.

Istraživanja navode da su brendovi živi i veoma prisutni na Internetu, kao i da su potrošači voljni da plate najviše cene za proizvode i servise koje smatraju različitim.

7.3 TEHNOLOGIJE INTERNET MARKETINGA

Internet marketing ima iste ciljeve kao i klasični marketing, ali ima svoje specifičnosti. Glavni uticaji Interneta na tehnologije marketinga su (1) proširenje obima marketinških komunikacija, (2) povećanje bogatstva marketinških komunikacija i (3) veliko povećanje intenziteta tržišnih informacija.

Tehnologije Internet marketinga obuhvataju [1]:

1. Dnevnike Web transakcija (za čiju analizu se koristi OLTP - Online Transaction Processing; OLAP - *On Line Analysis Processing*);
2. Kolačići (*cookies*) i Web bagovi (*Web bugs*);
3. Baze podataka (DB), skladišta podataka (DW) i istraživanje podataka (*data mining*);
4. Mreže za oglašavanje (*Advertising Networks*), npr. NAI-*Network Advertising Initiative;*
5. Sistemi za upravljanje odnosima s kupcima (CRM - *Customer Relationship Menagament*).

1. Dnevnici Web transakcija

Dnevnici Web transakcija (*Web Transaction Logs*) ugrađeni su u softver Web servera, koji snima korisničke aktivnosti na nekom Web sajtu.

Dnevnici transakcija mogu da obezbede dragocene informacije za marketing, posebno kad su kombinovane sa formama za registraciju, koje se koriste za prikupljanje ličnih podataka i bazom podataka korpe za kupovinu, koja prikuplja podatke o izabranoj robi, kupovini i plaćanju. Omogućava da se ustanove glavni obrasci interesovanja kupaca i načini kupovine, npr. na koju stranicu korisnici prvo prelaze nakon osnovne stranice sajta, gde nakon toga i slično.

Vodeći alat za analizu dnevnika transakcija je *WebTrends* [1]. Na slici je primer dnevnika Web transakcija [1].

```
64.88.16.67 - - [13/May/2003:12:51:53 -0400] "GET /images/ebook.gif HTTP/1.1" 304 1313
"http://www.azimuth-interactive.com/landingpage_access.php?item=50018&source=
overturemsa&" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; Q312461)"
64.88.16.67 - - [13/May/2003:12:51:54 -0400] "GET /images/bookmarkusart.gif HTTP/1.1" 200
363 "http://www.azimuth-interactive.com/landingpage_access.php?item=50018&source=
overturemsa&" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; Q312461)"
64.88.16.67 - - [13/May/2003:12:51:54 -0400] "GET /images/smallazimuthlogo.gif HTTP/1.1" 200
2695 "http://www.azimuth-interactive.com/landingpage_access.php?item=50018&source=
overturemsa&" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; Q312461)"
64.88.16.67 - - [13/May/2003:12:51:54 -0400] "GET /images/trustseal_small.gif HTTP/1.1" 200
937 "http://www.azimuth-interactive.com/landingpage_access.php?item=50018&source=
overturemsa&" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; Q312461)"
64.88.16.67 - - [13/May/2003:12:51:54 -0400] "GET /images/OrderByPhone.gif HTTP/1.1" 200
2017 "http://www.azimuth-interactive.com/landingpage_access.php?item=50018&source=
overturemsa&" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; Q312461)"
64.88.16.67 - - [13/May/2003:12:51:54 -0400] "GET /images/credit.jpg HTTP/1.1" 200 12177
"http://www.azimuth-interactive.com/landingpage_access.php?item=50018&source=
overturemsa&" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; Q312461)"
```

Slika 7.8 Izvod iz dnevnika Web transakcija u trajanju od 2 sekunde

Pregled tipičnih podataka iz dnevnika transakcija prikazan je u tabeli 7.2.

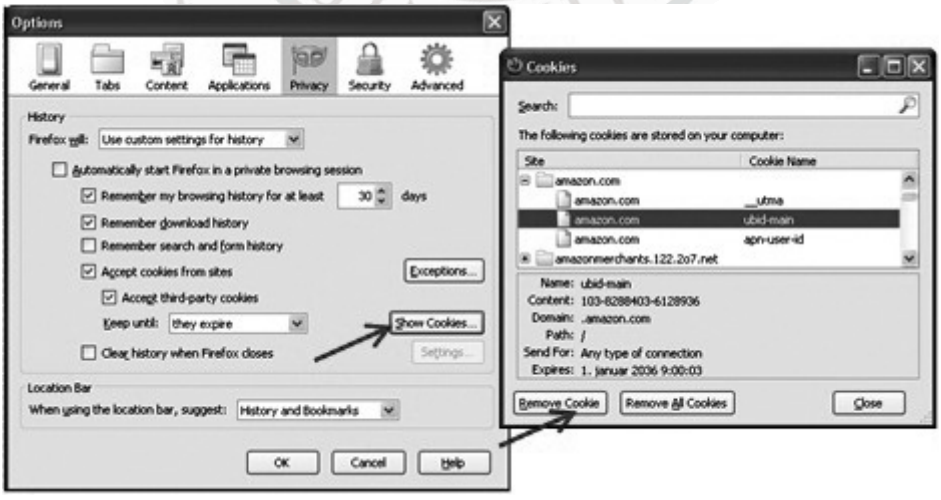
Tabela 7.2 Tipična upotreba podataka iz Web dnevnika u marketingu

Podatak	Upotreba u marketingu
IP adresa posetioca: 64.88.16.67	Za slanje povratnih marketinških poruka e-pošte korisnicima koji imaju stalnu URL adresu, dok se za modemske korisnike ne koriste, jer imaju privremene adrese
Datum i vreme aktivnosti: [1 3/May12003:—1 2:51:53 _0400J	Za otkrivanje vremenskih obrazaca ponašanja
Zahtevane i posećene stranice i objekti (naredbe *Get*): GET /images/ebook.gif	Za razumevanje šta je korisnika konkretno zanimalo u odgovoru (niz klikova). Može se kasnije koristiti za slanje personalizovanih poruka ili povratnih poruka o pregledanim proizvodima
Odgovor servera sajta: 200	Za nadgledanje pokidanih veza

Podatak	Upotreba u marketingu
Veličina poslane stranice (bytes): 1313	Za razumevanje potrebnog kapaciteta servera i komunikacija
Naziv stranice ili sajta s kojeg potrošač dolazi: http://www.azimuth-interactive.coml landingpage_access. php ?item=500 1 8&source=overturemsa”	Za razumevanje načina dolaska potrošača na sajt i obrasca njegovog ponašanja na posmatranom sajtu
Naziv i verzija upotrebljenog Web čitača: Mozilla/4.0 compatible; MSIE 6.0 (*Mozilla* je Netscape standard, a *MSIE* je Microsoft Internet Explorer)	Za otkrivanje ciljnog čitača, radi potvrde da je sajt kompatibilan sa korišćenim čitačima
Naziv i verzija operativnog sistema klijentskog računara potrošača: Windows 98	Za otkrivanje mogućnosti klijentskog računara, gde savremeniji operativni sistem znači novi računar ili tehnički obrazovanijeg klijenta
Istorija svih stranica i posećeni objekti u toku sesije	Za obezbeđenje ličnih profila pojedinaca, analizu aktivnosti sajta i otkrivanje najpopularnijih stranica i resursa

2. Kolačići i Web bagovi

Kolačići (*cookies*) su mali tekst fajlovi, koje Web sajtovi postavljaju na klijentski računar posetioca svaki puta kada poseti Web sajt i pristupa određenim stranicama. Omogućavaju agentima Web marketinga vrlo brz način za identifikaciju i ponašanje kupaca u prethodnom periodu. Lokacija ovih fajlova na računaru zavisi od operativnog sistema i Web čitača. Na slici je prikazan način upravljanja kolačićima (pregled i brisanje) u Web čitaču *Mozilla Firefox*.



Slika 7.9 Upravljanje kolačićima (*Mozilla Firefox* Show Cookies)

Web bagovi (*Web bugs*) su mali grafički fajlovi, koji se obično se sastoje samo od jednog piksela. Upotrebljavaju se za automatsko slanje informacija o korisniku i tekućoj Web stranici na server, radi nadgledanja. Ugrađuju se u Web stranice i e-mail poruke na poseban način, korišćenjem posebne HTML naredbe koja označava hipervezu ka izabranom serveru. Tako male slike su praktično nevidljive za korisnika računara, a pristup serveru na kome se nalaze slike evidentira se slanjem više podataka o korisničkom računaru:

- IP addresa računara koji traži stranicu sa slikom (Web bagom)
- URL Web stranice u kojoj se nalazi Web bag
- URL Web baga
- vreme prikazivanja Web baga
- vrsta Web čitača koji preuzima Web bag
- prethodno postavljena vrednost kolačiča

Različiti tipovi Web bagova uključuju obične rasterske slike u formatu GIF, izvršne bagove i izvršne bagove koji se zasnivaju na skriptu.

Interesantan je i društveni aspekt upotrebe Web bagova. Dok marketinški stručnjaci tvrde da Web bagovi nisu opasni, zagovornici privatnosti postavljaju pitanje zašto se onda skrivaju.

Organizacije za zaštitu privatnosti, za korišćenje Web bagova preporučuju:

- da budu vidljivi i označeni tako da ukazuju na njihovu funkciju
- da identifikuju ime kompanije koja ih je postavila
- da prikazuju izjavu o podacima koje otkrivaju, ako se na njih klikne
- da omoguće korisniku opciju njihovog uklanjanja

Za sada nema zakonske regulative za korišćenje ove forme prikupljanja podataka o ponašanju Web korisnika. Inicijativa za reklamiranje preko mreže NAI (*Network Advertising Initiative*) naziva ih Web peciva (*Web beacons*) i izdaje svoja uputstva.

3. Baze i skladišta podataka i istraživanje podataka

Baza podataka (*Database*) je organizovani skup logički povezanih podataka smeštenih u računaru.

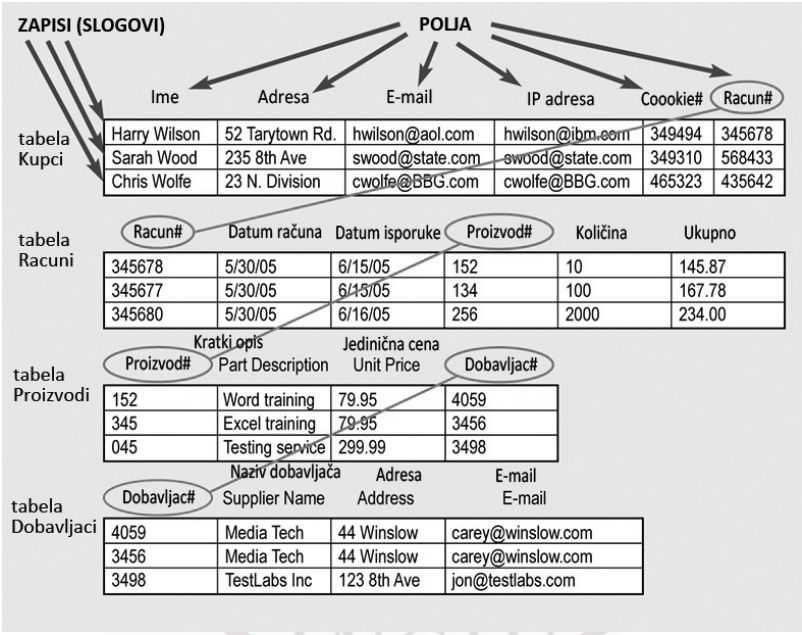
Sistem za upravljanje bazama podataka (*Database Management System*, DBMS) je softver koji se koristi za kreiranje, održavanje i pristup bazama podataka.

Relaciona baza podataka predstavlja podatke u obliku skupa dvodomenzionalnih tabela sa zapisima organizovanim u redove i atributima entiteta organizovanim u kolone; podaci različitih tabela se mogu međusobno povezivati, ako dele zajednički element podataka, koji se naziva primarni ključ (ili deo primarnog ključa).

Jezik SQL (*Structured Query Language*) je standardni jezik za postavljanje upita i manipulisanje bazom podataka, koji se koristi u relacionim bazama podataka.

Baze podataka

Na slici 7.10 prikazana je struktura jednostavne relacione baze podataka Web sajta e-trgovine, u kojoj su podaci o kupcima, proizvodima, dobavljačima i narudžbama (računima) smešteni i posebne tabele, povezane zajedničkim podacima (vezama, ključevima).



Slika 7.10 Primer jednostavne relacione baze podataka namenjene e-trgovini

Skladište podataka

Skladište podataka (*Data Warehouse*) je baza podataka u kojoj se na jednom mestu prikupljaju podaci o transakcijama firme i podaci o kupcima, radi kasnije *offline* analize stručnjaka za marketing i menadžera Web sajta.

Istraživanje podataka

Istraživanje podataka (*Data Mining*) je skup analitičkih tehnika za pronalaženje obrazaca u podacima, modela ponašanja kupaca i za razvoj profila kupaca.

Postoji više vrsta metoda istraživanja podataka:

- metodi koji se zasnivaju na upitima (*query driven*), koji koriste specifične SQL upite;

- metodi koji se zasnivaju na modelima (*model-driven*), koji uključuju korišćenje modela ponašanja i analiziraju ključne promenljive od interesa za donosioce odluka;
- metodi koji se zasnivaju na pravilima (*rule-based*), koji ispituju demografske i transakcione podatke grupa i pojedinaca na Web sajtu i nastoje da izvedu opšta pravila ponašanja posetilaca sajta;
- metodi kolaborativnog filtriranja (*collaborative filtering*), koji koriste bihevioristički pristup. Posetioci sajtova sami klasifikuju sebe u grupe sa istim afinitetima na bazi zajedničkih interesa, a proizvodi se zatim preporučuju na osnovu toga šta su drugi iz grupe nedavno kupovali.

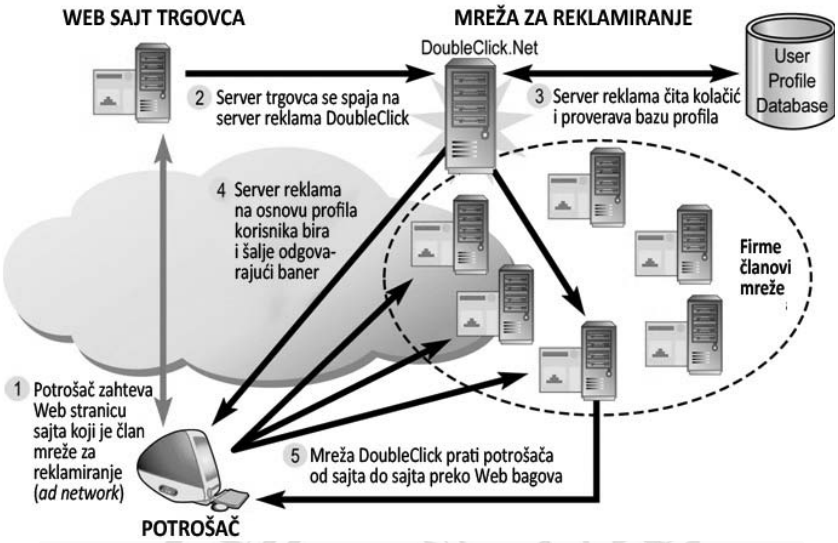
Slika 7.11 Istraživanje podataka i personalizacija

Kolaborativno filtriranje automatizuje proces sakupljanja i distribucije preporuka od drugih korisnika. Prvi pokušaji uvođenja automatizacije imali su brojne nedostatke: efekat prvog uvođenja, efekat slabe popularnosti, efekat pogrešnog izbora potrošača i dr. Rešenja uključuju uvođenje funkcije urednika (čoveka), koji traži od potrošača da uspostave svoje profile.

4. Mreže za reklamiranje

Mreže za reklamiranje (*Advertising Networks*) mogu da prikazuju korisnicima reklamne banere, na osnovu sadržaja baza podataka o ponašanju korisnika. Server za reklamiranje (*Ad server*) bira odgovarajuće banere na osnovu kolačića, Web bagova i profila iz baze podataka korisnika.

Najpoznatiji primer mreže za reklamiranje je *DoubleClick*. Na slici je prikazan način funkcionisanja mreže za reklamiranje kao što je *DoubleClick*.



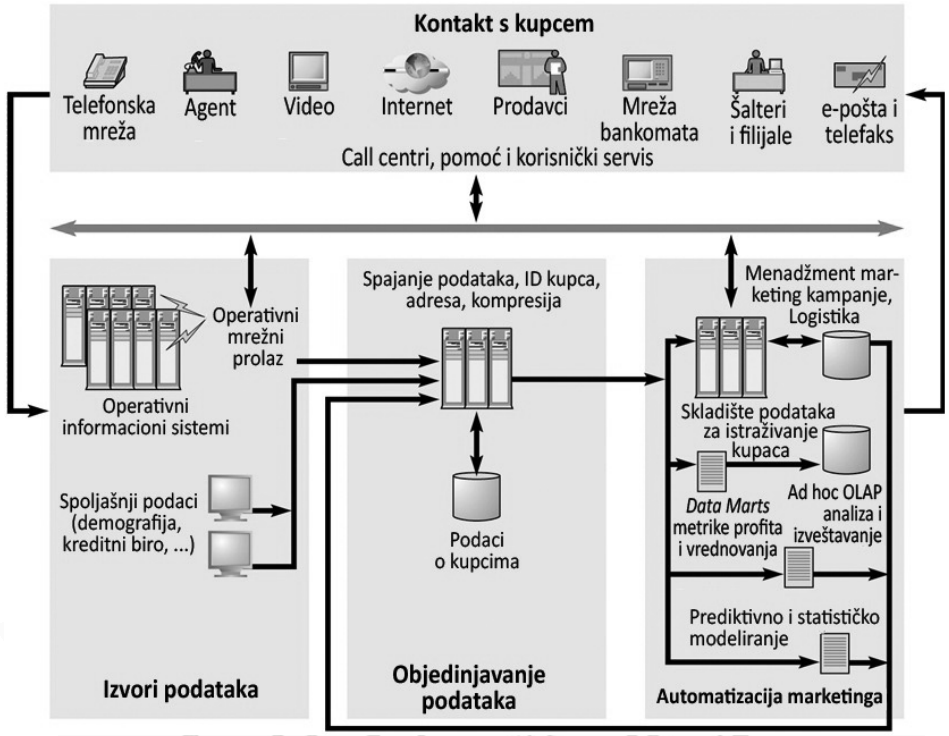
Slika 7.12 Funkcionisanje mreže za reklamiranje

5. Sistemi za upravljanje odnosima s kupcima

Sistemi za upravljanje odnosima s kupcima (*Customer Relationship Management Systems*, CRM) su skladišta informacija o klijentima, gde se beleže svi kontakti korisnika sa kompanijom i stvara profil klijenta, koji je dostupan svima u kompaniji koji treba da poznaju kupca (*know the customer*). Korisnički profili mogu da sadrže:

- kartu odnosa klijenta sa firmom
- rezime podataka o proizvodima i njihovoj upotrebi
- demografske i psihološke (psihografske) podatke
- mere profitabilnosti
- istorijat kontakata
- informacije o marketingu i prodaji

Na slici je prikaz strukture sistema za odnose s kupcima (CRM).



Slika 7.13 Sistem za odnose s kupcima (CRM)

7.4 STRATEGIJE B2C I B2B MARKETINGA I BRENDIRANJA U E-TRGOVINI

Nove tehnologije Internet marketinga dovele su do razvoja novih marketinških tehnika i poboljšanja efekata postojećih. Opisaće se strategije Intenet marketinga za ulazak na tržište, privlačenje i zadržavanje kupaca, određivanje cena i rešavanje konfilkata u prodajnim kanalima, koje su primenjive i na B2C i B2B forme e-trgovine.

7.4.1 Strategije Internet marketinga za ulazak na tržište

Osnovne strategije ulaska firme na tržište prikazane su na Slici 7.14, kao i primeri kompanija e-trgovine koje su ih upotrebile.

Slika 7.14 Generičke strategije ulaska na tržite

Nove firme su se u prvoj fazi razvoja e-trgovine bavile isključivo online trgovinom, koristeći strategiju prvog pokretača (*First mover*).

Njihovi neposredni sledbenici bile su postojeće kompanije, koje su iskoristile priliku da uz relativno mala ulaganja uđu na novo tržište (*Fast folower*). Sve online kompanije su za izgradnju svog novog brenda ulagale u široku marketinšku kampanju u tradicionalnim medijima.

Neke nove kompanije, koje su se istovremeno opredelile za online i tradicionalno poslovanje, za ulazak na tržište su iskoristile savezništvo sa firmama koje su već izgradile svoj brend u tradicionalnom poslovanju (*Alliances*).

Postojeće tradicionalne kompanije uglavnom proširuju svoje poslovanje na novo tržište, tako što koriste i proširuju svoj postojeći brend (*Brand extender*).

7.4.2 Uspostavljanje odnosa sa kupcima

Nakon izbora marketinške strategije, prelazi se na uspostavljnaje odnosa sa kupcima. Osnovna sredstva za uspostavljanje svesti o kompaniji su tradicionalni odnosi s javnošću i reklamni mediji, kao što su štampa, direktna pošta, televizija i radio, ali su se pojavile i nove, uspešne tehnike Internet marketinga:

Marketing sa dozvolom (Permission Marketing)

Strategija marketinga u kojoj kompanija dobija dozvolu od kupaca pre slanja informacija ili promotivnih poruka kupcu. Primer je *opt-in* e-mail, termin koji se koristi kada se nekome nudi mogućnost da primi *bulk e-mail*, e-poštu koja se šalje mnogim ljudima u isto vreme. To je obično neka vrsta liste slanja, biltena ili reklame. Dobijanje dozvole pre slanja e-maila je kritično, jer bez nje je to neželjena masovna e-pošta, poznatija kao *spam*.

Marketing partnera (Affiliate Marketing)

Marketing partnera je strategija marketinga koja se oslanja na reference, tako što se jedan Web sajt slaže da plaća proviziju drugom Web sajtu za nove poslovne šanse prvog sajta.

Marketing sa preporukom (Viral Marketing) na Web-u 2.0

Marketing sa preporukom je proces obezbeđivanja spremnosti kupaca da prosleđuju markentiške poruke kompanije prijateljima, familiji i kolegama (tzv. *multilevel marketing*).

Blog Marketing

Forma marketinga, u kojoj kompanije koriste blogove za marketing kroz dijalog s kupcima o svojstvima svojih proizvoda i usluga.

Mrežni marketing i kupovina preko društvenih mreža

Mrežni marketing preko društvenih mreža (*Social Network Marketing*) koristi razmenu stavova i ideja na postojećim društvenime mrežama za komercijalno objavljivanje proizvoda.

Grupna kupovina (*Social Shopping*) je forma e-kupovine u koju se uključuju i dugi članovi grupe koji komuniciraju putem društvene mreže.

Podsticaj brendom (Leveraging Brands)

Podsticaja brendom je proces korišćenja moći postojećeg brenda za dobijanje novih kupaca za novi proizvod ili servis.

7.4.3 Zadržavanje kupaca

Tehnike Internet marketinga omogućavaju uspostavljanje tesnih veza s kupcima i diferencijaciju proizvoda i usluga. Klasične strategije obuhvataju masovni marketing, direktni marketing i mikromarketing.

Masovni (Mass) marketing

Pristup u kome se ne vrši segmentacija, već se za obraća velikoj grupi kupaca na nacionalnom nivou (Tide, McDonalds).

Direktni (Direct) marketing

Direktna pošta ili telefonski kontakt u okviru segmenta potencijalnih ili lojalnih kupaca.

Mikromarketing

Marketing na osnovu baze podataka potencijalnih kupaca formirane prema uskom geografskom ili tehnološkom kriterijumu.

Personalizovani 1:1 marketing

Personalizovani, 1:1 marketing uključuje segmentiranje tržišta prema preciznom i blagovremenom razumevanju individualnih potreba, usmeravanje specifičnih marketinških

poruka ovim pojedincima i pozicioniranje proizvoda u odnosu na konkurente tako da bude istinski jedinstven.

Personalizacija može povećati kod potrošača osećaj kontrole i slobode, ali može da prozrokuje neželjeni osećaj gubitka anonimnosti.

Kastomizacija i koprodukcija

Kastomizacija je promena proizvoda (ne samo markentiških poruka) prema željama korisnika. Ko-produkcija dopušta kupcu da interaktivno kreira proizvod (primer su beta verzije softverskih proizvoda).

Transaktivni sadaržaj

Najčešći razlog za pristup Internetu je slanje e-pošte i pronalaženje informacija, pa su tako prilagođene i strategije marketinga koje korisniku nude transaktivni sadržaj, rezultat kombinacije tradicionalnih sadržaja (prikazi proizvoda) sa dinamičkim informacijama (najave novih proizvoda) u skladu sa profilom kupca.

Korisnički servis

Servisni alati za podršku korisnika uključuju:

- najčešće postavljana pitanja (FAQs) - lista opštih tekstualnih pitanja i odgovora;
- sisteme za servis ćaskanja (*chat*) kupaca u realnom vremenu (tehnologije inteligentnih agenata, *bot*-ova);
- Sisteme sa automatizovanim odgovorima, koji šalju potvrde o prijemu e-pošte i priznanja.

Internet strategije formiranja cena

Strategija formiranja cena je deo marketinga. Cena i kvalitet određuju vrednost proizvoda na tržištu. Za određivanje cene se, osim fiksnih i varijabilnih troškova, uzima u obzir i kriva tražnje, odnosno procena količine proizvoda koja se može prodati po određenoj ceni. Segmentacija tržišta omogućava diskriminaciju cena, odnosno prodaju po ceni koju je neko spreman da plati, čime se maksimizuje prodaja i profit.

Osnovne strategije određivanja cena su: besplatno ustupanje (*freee*), prodaja verzija istog proizvoda po različitim cenama (*Versioning*), prodaja različitih prozvoda po istoj ceni (Bundling) i dinamičko ili aukcijsko određivanje cena (*Dynamic Pricing*).

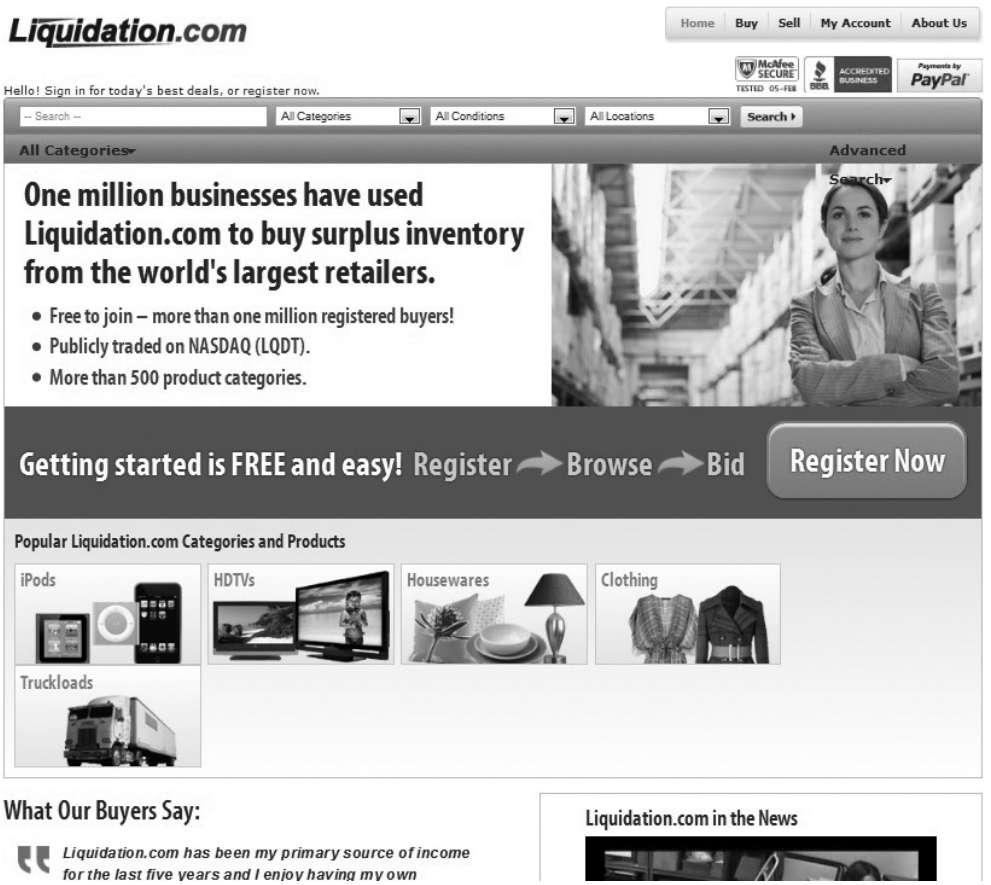
Upravljanje konfliktima u prodajnim kanalima

Kanali (*channels*) predstavljaju različite metode distribucije i prodaje proizvoda, kao što su direktna prodaja, prodaja preko posrednika (distributera i maloprodaje) ili e-prodaja. Konflikti nastaju kada se pojavi nova mogućnost prodaje prozvoda ili usluge, koja može da naruši prodaju postojećeg (npr. prodaja muzike preko Interneta narušava tradicionalnu maloprodaju).

Proizvođači često odustaju od direktne prodaje, koju prepuštaju alternativnim prodajnim kanalima (automobili, računari, putovanja) ili prodaju vrše po modelu partnerstva, odvajajući deo Internet prodaje za podršku maloprodajnoj mreži i plaćanje usluga dostave i održavanja.

Ilustracija: Liquidation.com - primer uspešnog B2B marketinga

Kompanija Liquidation.com ima B2B aukcijski model poslovanja, koji je usmeren na likvidirane robe. Na Slici 7.15 vidi se osnovna stranica Web sajta, sa reklamom same kompanije i kratkim uputstvom za upotrebu.

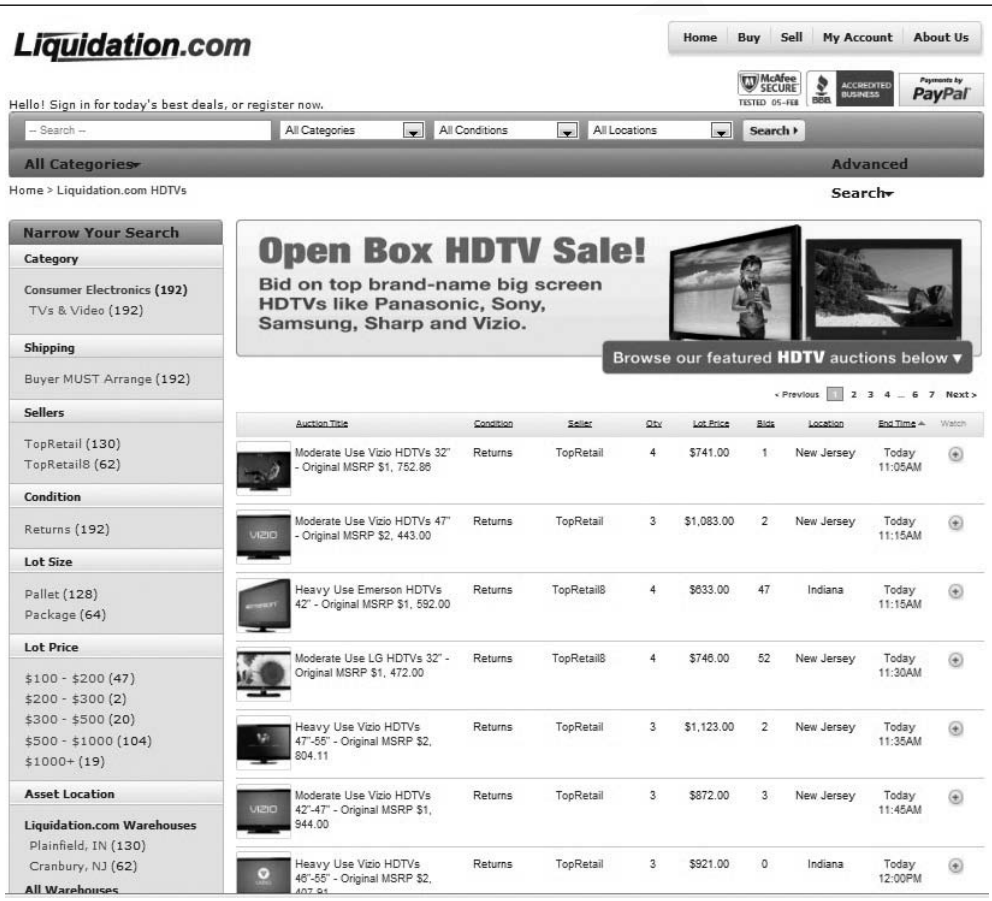


Slika 7.15 Osnovna stranica kompanije sa reklamama i uputsvima

Prodaja roba likvidiranih kompanija, koje nisu vlasništvo liquidation.com, vrši se putem aukcija, koje se organizuju svaka 2-3 dana na sličan način kao na sajtu eBuy.com. Osnovni problem marketinga je stalna promena i nepredvidivost ponude proizvoda.

Tehnike marketinga i brendiranja koje je kompanija koristila za uspostavljanje globalnog i pouzdanog brenda u posebnoj oblasti e-trgovine obuhvataju:

- izgradnju poverenja kroz udruživanje i stalnu brigu o kupcima - da uvek roba bude ispravna i isporučena ili da se novac vrati;
- analizu dnevnika Web transakcija, formulare za registraciju kupaca;
- marketing pretraživačem (Google i Overture);
- nekonvencinalne niskobudžetske kampanje za odnose sa javnošću (guerilla marketing) i ograničeno reklamiranje;
- nenametljivi e-mail marketing.



Slika 7.16 Katalog robe sa baner reklamom

7.5. LITERATURA

[1] Laudon K.C., Traver C.G., *E-commerce, business, technology, society*, 3rd Ed, Addison Wesley, 2006

[2] USC Annenberg School Center for Digital Feature, *World Internet Project: International Report 2010*, 2011 http://www.digitalcenter.org/WIP2010/wip2010_long_press_release_v2.pdf

[3] Zickuhr K., *Generations and their gadgets*, Pew Report, 2011. http://pewinternet.org/~/media//Files/Reports/2011/PIP_Generations_and_Gadgets.pdf

[4] Pres saopštenje, *Upotreba informaciono- komunikacionih tehnologija u Republici Srbiji, Republički zavod za statistiku*, 2010. http://webrzs.stat.gov.rs/axd/dokumenti/ict/2010/Saop2010.pdf

[5] www.stat.gov.rs

[6] www.marketingterms.com

[7] www.merriam-webster.com

[8] www.wikipedia.org

[9] www.whatis.com

[10] www.internet2.edu

8. MARKETINŠKE KOMUNIKACIJE U ELEKTRONSKOJ TRGOVINI

U ovom poglavlju se izlažu osnovne tehnike marketinških komunikacija u elektronskoj trgovini, razmatra se njihova isplativost i načini upotrebe Web sajta e-trgovine kao alata za marketinške komunikacije.

8.1 MARKETINŠKE KOMUNIKACIJE

Online marketinške komunikacije su metodi koje koriste *online* firme za komunikaciju sa potrošačima i kreiranje brendova. Tu spadaju:

- Promotivne prodajne komunikacije sugerišu potrošaču da kupuje odmah i prave takve ponude da ohrabre neposrednu kupovinu;
- Komunikacije za brendiranje usmerene su na promociju diferencijalnih prednosti potrošnje određenih proizvoda ili servisa i retko sugerišu potrošaču da kupuje odmah.

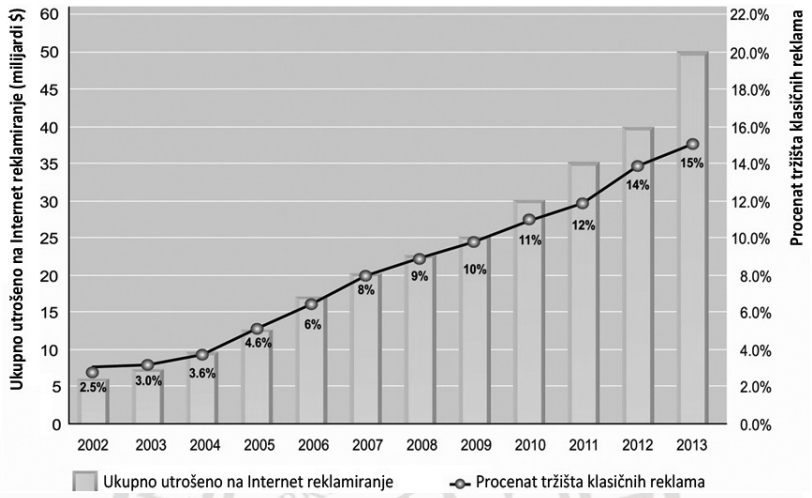
Postoje brojne forme online marketiških komunikacija, kao što su online reklamiranje, e-mail marketing i odnosi s javnošću.

8.1.1 Online reklamiranje

Online reklamiranje (*advertising*) obuhvata plaćene poruke na Web sajtu, online servisu ili drugom interaktivnom medijumu, kao što je interaktivna razmena poruka. Ulaganja u ovaj vid reklamiranja su u stalnom porestu, Slika 8.1 [1]. Godine 2007. na online reklamiranje utrošeno je 21,4 milijaradi dolara, dok su ulaganja u 2010. dostigla 30 milijardi, s tendencijom daljeg rasta.

Prednosti online reklamiranja su mogućnost usmeravanja reklame na uske segmente tržišta (ciljne grupe), praćenje performansi skoro u realnom vremenu i obezbeđenje veće šanse za interaktivni rad.

Nedostaci ovog načina reklamiranja su neizvesna isplativost (*cost*/*benefit*) i teškoće adekvatnog merenja rezultata.



Slika 8.1 Ulaganja u online reklamiranje od 2000 do 2013

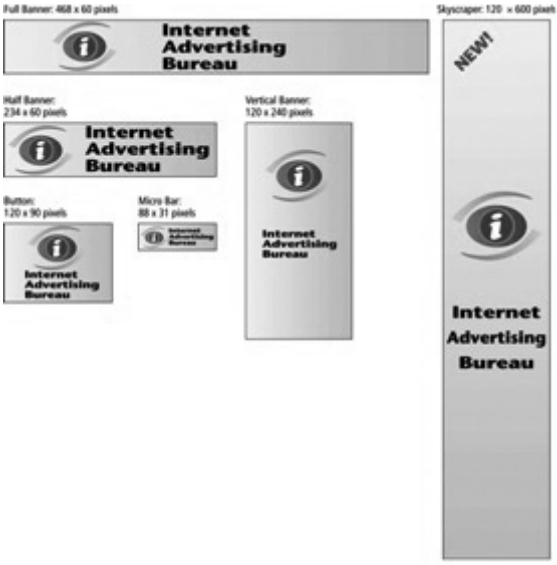
Glavne forme online reklamiranja su: ekranske i multimedijske reklame (*display ads*, *rich media ads*), marketing pretraživačem (*search engine*), sponzorstvo i preporuke putem partnerskih odnosa (*affiliate relationships*).

Ekranske reklame

U ekranske reklame (*display ads*) spadaju:

- Baneri (*banners*), koji prikazuju promotivne poruke u pravougaonom boksu na vrhu ili dnu ekrana monitora;
- Iskačući prozori (*pop-ups*), koji se javljaju na ekranu bez korisničkog aktiviranja;
- Zaklonjeni prozori (*pop-unders*), koji se otvaraju ispod aktivnog prozora korisničkog čitača i ne pojavljuju se dok korisnik ne zatvori aktivni prozor.

Baner reklame su najstariji oblik Internet reklamiranja. Obično se realizuju kao male digitalne (rasterske) slike, za koje je preporuke standardnih formata dala organizacija Biro za interaktivno reklamiranje (*Interactive Adveritsing Bureau*, IAB) [1], Slika 8.2.



Slika 8.2 Tipovi baner reklama

Metodi postavljanja online reklama su:

- Razmena banera (*banner swapping*), koja predstavlja aranžman između firmi i dopušta svakoj firmi da ima svoj baner postavljen na drugim partnerskim sajtovima bez naknade;
- Reklamne mreže (*advertising exchanges*), koje deluju kao brokeri između oglašavača i izdavača, koje postavljaju reklame i prate sve aktivnosti koje se na njih odnose.

Multimedijske reklame

Multimedijske reklame (*rich media/video ads*) koriste multimedijske sadržaje, kao što su animacije i video u formatima Flash, DHTML, Java, *streaming audio* ili *video*. Više se koriste us svrhu brendiranja nego same prodaje.

Dok baneri zauzimaju mali deo ekrana stranice, multimedijske reklame su različitih dimenzija i mogu da zauzimaju celu Web stranicu. Prema načinu postavljanja, mogu biti:

- Umetnute stranice (*Interstitials*) su cele stranice poruka između tekuće stranice i stranice na koju korisnik želi da pređe;
- Pridodate stranice (*Superstitials*) su multimedijske reklame, koje su prethodno preuzete u keš klijentskog Web čitača i ne prikazuje se sve dok se potpuno ne preuzmu i korisnik ne pređe na drugu stranicu.

Marketing pretraživačem

Marketing pretraživačem (*search engine marketing*) jedna je od najbrže rastućih i najefektivnijih formi online marketinških komunikacija. Udeo ovog načina oglašavanja narastao je od 1% u 2000. godini do 40% u 2010. godini [1].

Marketing pretraživačem obuhvata:

- Plaćeno uključivanje (*Inclusion*), gde firme plaćaju za uključivanje sajta u indeks pretraživača;
- Plaćeno postavljanje (*Placement*), gde firme plaćaju za garanciju da će se reklama uočljivo pojaviti za svako relevantno pretraživanje.

Pretraživači *Google*, *Yahoo* i *MSN* su vodeće kompanije u ovoj tehnologiji.

Problemi koji prate ovaj način reklamiranja su:

- razotkrivanje plaćenog uključivanja i prakse postavljanja neke reklame
- zloupotreba trećih lica radi radi zlonamernog pokretanja reklama i stvaranja troškova (*search engine click fraud*);
- neodgovarajuće reklame (*Ad nonsense* - Google *AdSense* reklame koje ne odgovaraju sadržaju stranice).

Sponzorstvo

Sponzorstvo je plaćeno povezivanje imena oglašavača sa određenom informacijom ili događajem na pozitivan način, koji pojačava brend, ali još uvek ne na otvoreno komercijalan način (uobičajena forma oglašavanja).

Partneske preporuke

Predstavljaju način reklamiranja gde se partnerskoj firmi dozvoljava da postavi svoj reklamni logotip ili reklamni baner na Web sajt druge partnerske firme, preko kojeg se korisnici mogu povezati na njen sajt. Ponekad se nazivaju i ugovori o iznajmljivanju.

Na slici 8.3 prikazan je prostor na sajtu *Amazon.com* rezervisan ta ugovorene reklame (*More Items to Consider*), koji koristi kompanija *ToysRUs*.com (ToysRUs).

Slika 8.3 Partnerska reklama kompanije ToysRUs.com na sajtu Amazon.com

Problem u ovakvom načinu reklamiranja je mogućnost kidnapovanja kupaca.

8.1.2 E-mail marketing

Direktni e-mail marketing je slanje e-mail marketing poruka direktno zainteresovanim kupcima koji su se odlučili ili onima koji se još nisu odlučili.

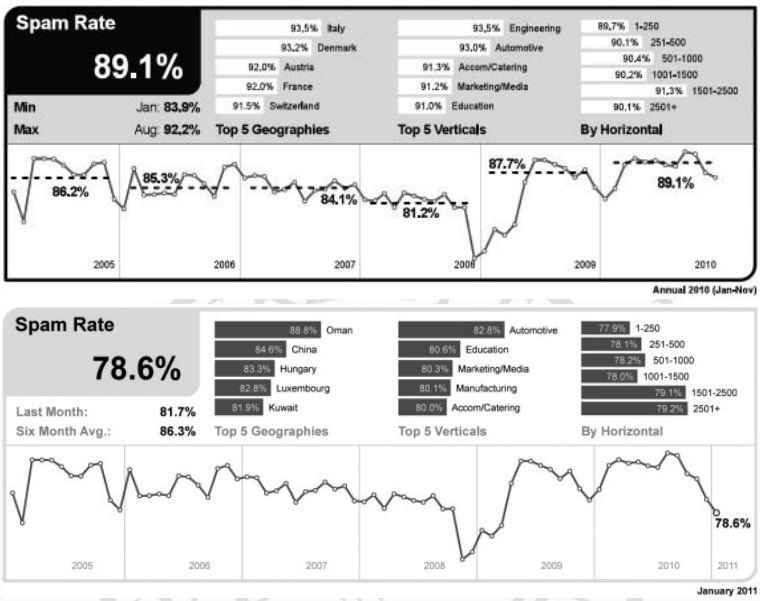
Neželjena pošta (*spam*) je neželjeni komercijalni e-mail. Spam se širi bez kontrole, oko 70-80% svih namenskih Internet e-mail poruka spada u ovu kategoriju.

Načini kontrole neželjene komercijalnih poruka e-pošte obuhvataju:

- Upotrebu softvera za filtriranje (*fiewalls*), koji je samo delimično efektivan, jer kompanije koje koriste ovaj vid oglašavanja finansiraju razvoj tehnika za njihovo prevazilaženje;
- Samoregulaciju industrije, odnosno mere i akcije marketinških udruženja i organizacija, koje nisu dale velike rezultate;
- Državnu regulaciju, koja je neophodna, ali u većini zemalja u svetu nema odgovarajućeg zakona.

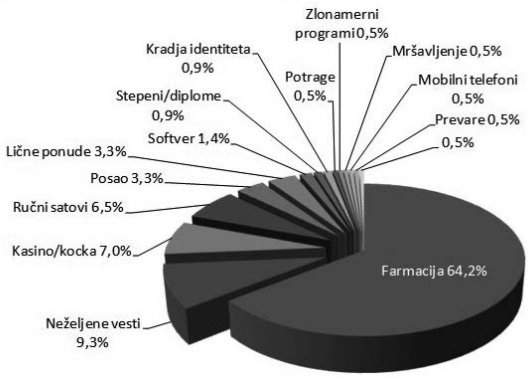
Na slici 8.4 [2] prikazani su osnovni statistički podaci o udelu neželjene komercijalne e-pošte u ukupnom prometu na kraju 2010. godine, kao i promene za period od 2005 do januara 2011. Na kraju godine udeo neželjene pošte iznosio je 78,6% [3], dok je prosek za 2010. godinu bio čak 89,1%.

Najveći udeo zabeležen u nekoliko evropskih zemalja (preko 90%), dok su među najzastupljenijim delatnostima proizvodnja, edukacija i marketing.



Slika 8.4 Udeo neželjenih komercijalnih poruka elektronske pošte (2005-2010)

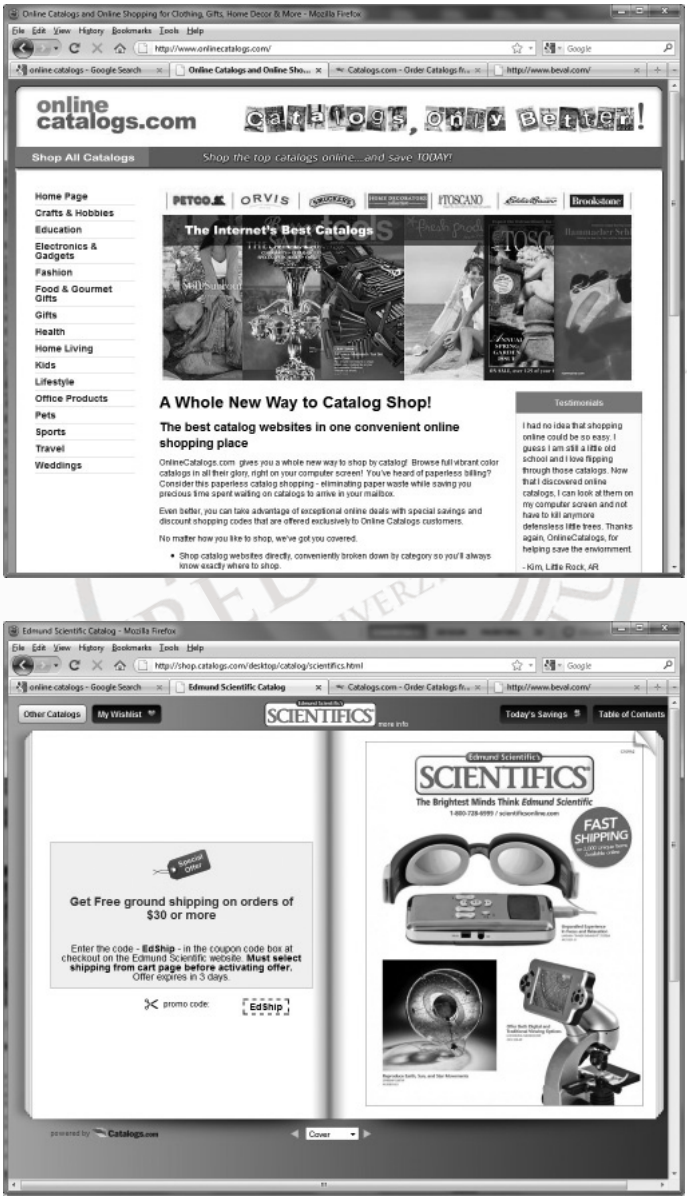
Na Slici 8.5 prikazane su osnovne kategorije neželjenih poruka, koje su formirne na osnovu podataka iz 2010. godine. Vidi se da je gotovo dve trećine poruka povezano sa famaceutskim kompanijama, dok je jedan mali deo zlonameran.



Slika 8.5 Kategorije neželjenih poruka (spam)

8.1.3 Online katalozi

Online katalozi predstavljaju ekvivalent papirnih kataloga. Popularnost i upotreba rastu sa povećanjem brzine Interneta, pošto se sastoje od kvalitetnih fotografija u boji visoke rezolucije, Slika 8.6.



Slika 8.6 Primer online kataloga

Mnoge online kompanije koriste istovremeno i online i klasične kataloge, koje šalju elektronskim putem, pošto su istraživanja pokazala povoljan uticaj oba načina komunikacije na svest o brendu kompanije.

8.1.4 Društveni marketing

Društveni mediji su pristupačni svim korisnicima Interneta. Povećan obim komunikacije povoljno utiče na promovisanje brendova i povećanje kvaliteta usluga. Društvene mreže, kao što *Twitter* i *Facebook*, predstavljaju pogodne platforme za jeftinije sprovođenje marketinških kampanja.

Blog reklamiranje

Ovaj vid online reklama vezan je za sadržaj blog-ova i mišljenja i preporuke njihovih autora. Karakteristika autora i čitalaca blogova je da su to obično obrazovaniji, s većim primanjima i da dosta utiču na stvaranje javnog mnenja.

Reklamiranje putem društvenih mreža

Vrši se pooću reklame koje se postavljaju na sajtove društvenih mreža, kao što su *MySpace*, *Facebook* i *YouTube*.

Reklamiranje preko igara

Ovaj vid reklamiranja se zasniva na ponudama za preuzimanje reklamnih igara (*advergames*) u kojima se na vidnim mestima koristi ime određenog brenda.

Veza tradicionalnih i online marketinških komunikacija

Tradicionalni *offline* marketing orijentisana je na kupca i koristi Web za proširenje imidža brenda i prodajne kampanje. S druge strane, *online* kompanije koriste tradicionalne marketinške komunikacije za prodaju preko Web sajta. Najuspešnije marketinške kampanje ugrađuju *online* i *offline* taktike.

8.2 ISPLATIVOST ONLINE MARKETINŠKIH KOMUNIKACIJA

Online marketing je samo mali deo ukupnih marketinških komunikacija. Jedan od problema je ocena efekata online marketinga i određivanje isplativosti online reklamiranja.

8.2.1 Metrike online marketinga

Metrike online marketinga se odnose na uspešnost Web sajta u privlačenju posetilaca i pretvaranju posetilaca u potrošače, kao i komunikaciju putem e-maila.

Metrike usmerene na uspešnost Web sajta u privlačenju posetilaca ili udeo na tržištu:

- *Impressions*: broj prikazivanja neke reklame;
- *Click-through rate (CTR)* ili *View-through rate (VTR)*: procenat posetilaca koji su stvarno kliknuli/pogledali oglas;
- *Hits*: broj pogodaka (http zahteva);
- *Page views*: broj stranica koje su posetioci zahtevali;
- *Stickiness (duration)*: prosečno vreme zadržavanja posetioca na sajtu;
- *Unique visitors*: broj različitih posetilaca sajta;
- *Loyalty*: procenat posetilaca koji su se vratili na sajt u godini;
- *Reach*: procenat ukupnog broja potrošača na tržištu koji su posetili sajt;
- *Recency*: prosečan broj dana između poseta;

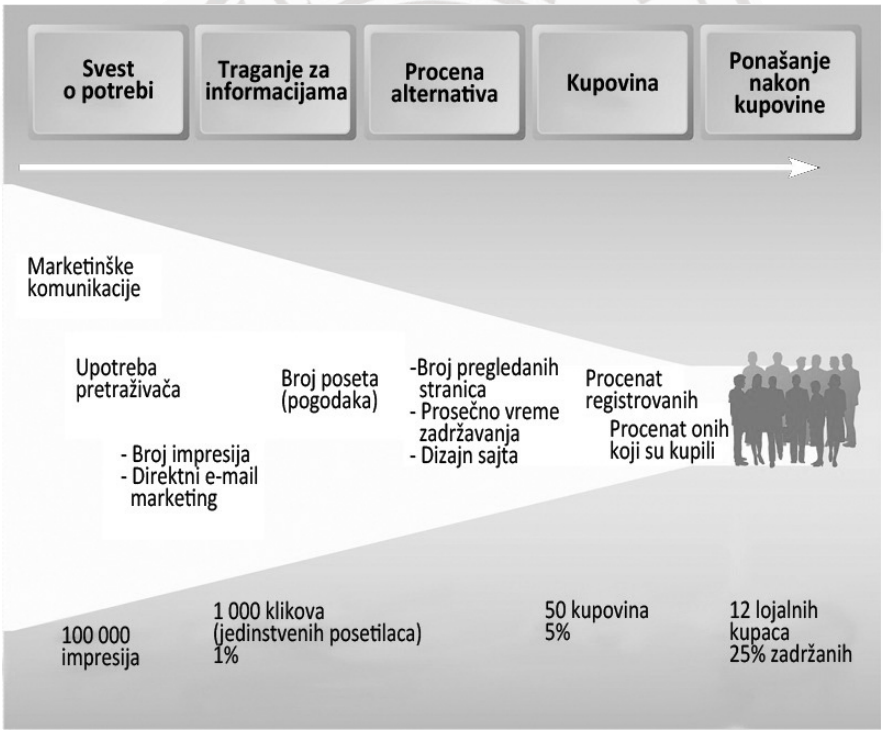
Metrike usmerene na pretvaranje posetioca u potrošača su:

- *Acquisition rate*: procenat posetilaca koji su se registrovali ili posetili stranice proizvoda;
- *Conversion rate*: procenat posetilaca koji su stvarno nešto kupili;
- *Browse-to-buy-ratio*: proceenat posetilaca koji pređu na kupovinu;
- *View-to-cart ratio*: procenat posetilaca koji uzme korpu;
- *Cart conversion rate*: procenat posetilaca koji uzme korpu i stvarno nešto kupi;
- *Checkout conversion rate*: procenat posetilaca koji su preduzeli ponuđenu akciju (kupovina, preuzimanje, pregled videa),
- *Abandonment rate*: procenat kupaca koji uzmu korpu za kupovinu, ali ne završe formular i napuste sajt;
- *Retention rate*: procenat postojećih kupaca koji nastave da regularno kupuju;
- *Attrition rate*: procenat kupaca koji su kupili jedanput, ali se nisu vratili u toku godine;

Metrike e-mail marketinga su:

- *Open rate*: broj kupaca koji je otvorio mail u e-mail kampanji;
- *Delivery rate*: procenat kupaca koji je primio poruku u e-mail kampanji (80% je dobro, dok je 90% i više vrlo dobro, a 100% gotovo nemoguće, zbog različitih sistemskih problema u razmeni elektronske pošte);
- *Click-through rate (e-mail)*: procenat odgovora ili klikova na veze u porukama e-pošte poslatim u kampanji;
- *Bounce-back rate*: procenat kupaca u kampanji koji nisu primili poruku, jer ih je vratio e-mail server ili klijent;
- *Unsubscribe rate*: procenat odjavljivanja kupaca iz liste u e-mail kampanji;
- *Conversion rate (e-mail)*: procenat kupaca koji su preduzeli ponuđenu akciju (kupovina, preuzimanje, pregled videa);

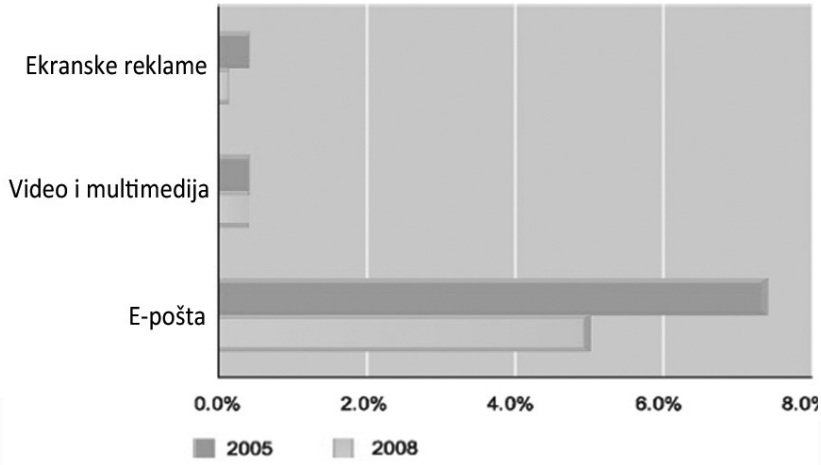
Na slici 8.7 prikazan je deo procesa kupovine i primena metrika marketinga u pojedinim fazama procesa kupovine.



Slika 8.7 Model online kupovine i metrike marketinga

8.2.2 Merenje efekta online reklamiranja

Iako broj poseta (klikova) nekom sadržaju može biti mali, u pitanju je samo jedna mera efektivnosti. Istraživanja navode da najmoćnije marketinške kompanije uključuju *online* i *offline* reklamiranje. Na Slici 8.8 prikazana je tipična posećenost pojedinih reklamnih sadržaja (*Click-through Rates*) na Web-u za period 2005–2008 [1].



8.8 Tipična posećenost reklamnih sadržaja (*Click-through Rates*) 2005–2008

8.2.3 Cena online reklamiranja

Glavni modeli određivanja cene online reklame su:

- *Cena po hiljadi impresija* (CPM), gde oglašavač plaća za prikazivanja-impresije od po 1.000 jedinica;
- *Cena ko kliku* (CPC), gde oglašavač plaća prethodno dogovorenu pretplatu za svaki klik koji reklama registruje;
- *Cena po akciji* (CPA), gde oglašavač plaća prethodno dogovoren iznos samo kada korisnik izvršava specifičnu akciju;
- *Hibridna cena*: istovremena primena dva ili više modela.

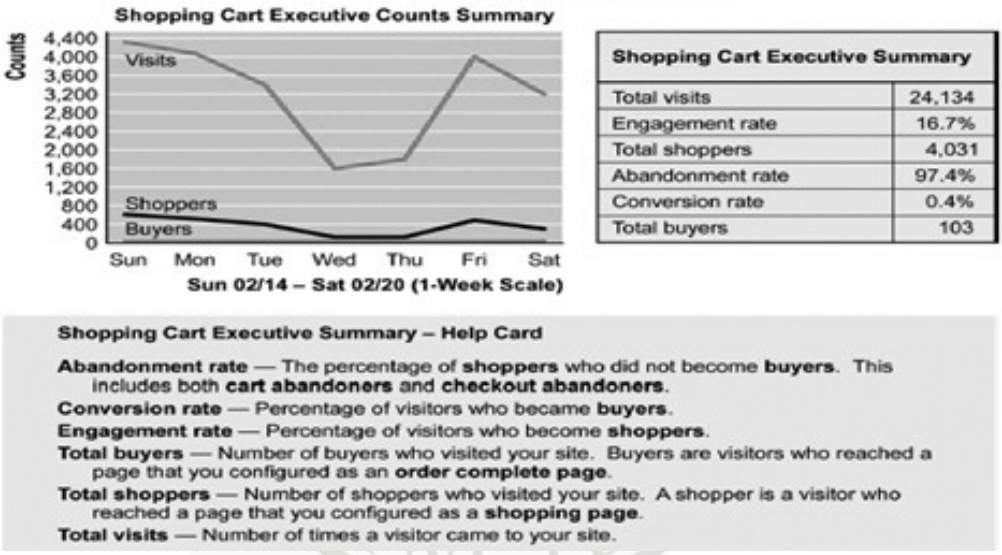
Načelno je *online* marketing na osnovu cene po hiljadi impresija (CPM) skuplji, ali efektivniji.

8.2.4 Softver za merenje rezultata online marketinga

Postoje brojni softverski alati za praćnje i analizu svih aktivnosti na Web sajtu. Najpoznatiji softverski alati za merenje rezultata marketinga su *Web Trends*, *WebSide Story* i *Google Analytics*.

WebTrends je softverski program koji automatski računa aktivnosti na sajtu, kao što su stopa napuštanja, stopa konverzije itd. *WebSideStory* je Web servis koji pomaže menadžerima marketinga.

Na Slici 8.9 je ilustracija skupa informacija koje analitički programi daju na osnovu analize aktivnosti na Web sajtu.



Slika 8.9 Analiza aktivnosti na Web sajtu

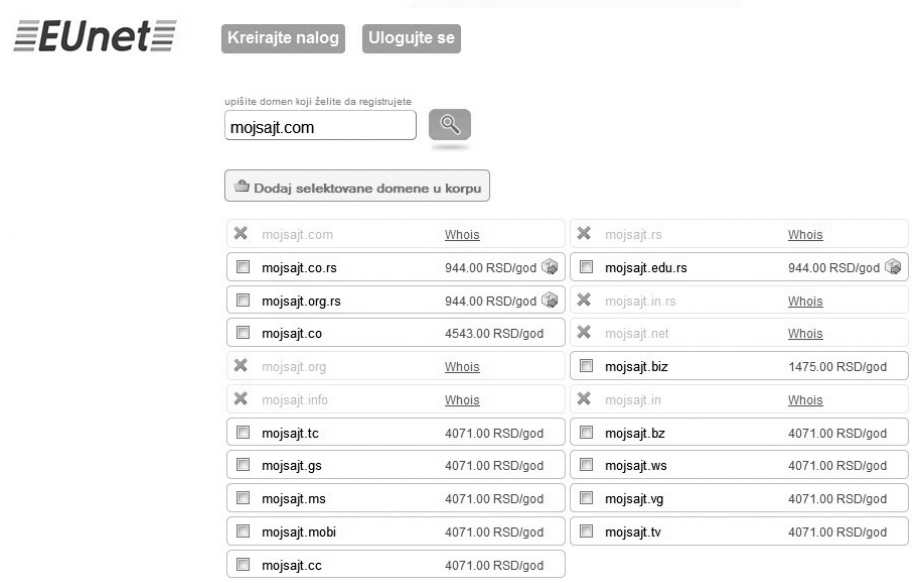
8.3 WEB SAJT KAO ALAT ZA MARKETINŠKE KOMUNIKACIJE

Funkcionalni Web sajt predstavlja jedno od najsnažnijih sredstava marketinških komunikacija, odnosno online reklamiranja. Na dobro dizajniranom Web sajtu korisnik može najlakše i najbrže da pronađe traženi proizvod ili dodatne informacije. Osim dizajna, važni elementi marketinške strategije su naziv domena i optimizacija za pretraživače (*search engine optimization*, SEO).

8.3.1 Nazivi domena

Prvu komunikaciju sa potencijalnim kupcem sajt e-trgovine ima preko imena domena (*domain name*), koji je deo njegove Web adrese. Poželjno je da ime domena bude kratko i karakteristično, da se lako pamti i da se ne zameni s nekim drugim. Ime ne mora da bude direktno vezano za poslovanje ili brend kompanije, ali su onda potrebna veća ulaganja u marketing.

Prilikom izbora naziva domena, treba koristiti mogućnost online provere zauzetosti naziva domena, koju obezbeđuju mnogi provajderi Internet usluga, koji nude usluge Web hostinga i posreduju u zakupu naziva domena. Na Slici 8.10 je primer rezultata provere jednog naziva domena *mojsajt*, zajedno sa godišnjom cenom zakupa. Zauzeti nazivi su posebno označeni, a slobodni se mogu zakupiti elektronskim putem.



Slika 8.10 Provera naziva domena

8.3.2 Optimizacija za pretraživače

Pošto pretraživače dnevno koristi ogroman broj korisnika Interneta, koji pregledaju samo mali broj odgovora na samom početku spiska odgovora koje dobiju od pretraživača, veoma je važno kako će se rangirati konkretan sajt kada se nađe zajedno sa nekim od drugih sajtova.

Pretraživači koriste posebne sopstvene programe za rangiranje Web stranica u odnosu na postavljeni kriterijum pretraživanja. Poznavanje njihovog načina rada i mogućnosti promocije Web sajta važan je deo projekta izgradnje Web sajta.

Opšte preporuke za optimizaciju Web sajta za pre postavljanja su:

- Registrovati se na što više pretraživača (*search engine*)
- Obezbediti da su ključne reči korišćene u opisu Web sajta iste one koje bi potencijalno korisnici mogli koristiti za pretraživanje
- Povezati sajt sa što više drugih sajtova
- Uzeti profesionalnu pomoć

8.3.3 Funkcionalnost Web sajta

Iistraživanja pokazuju da uspešnost Web sajta zavisi pre svega od kvaliteta sadržaja (*content is king*).

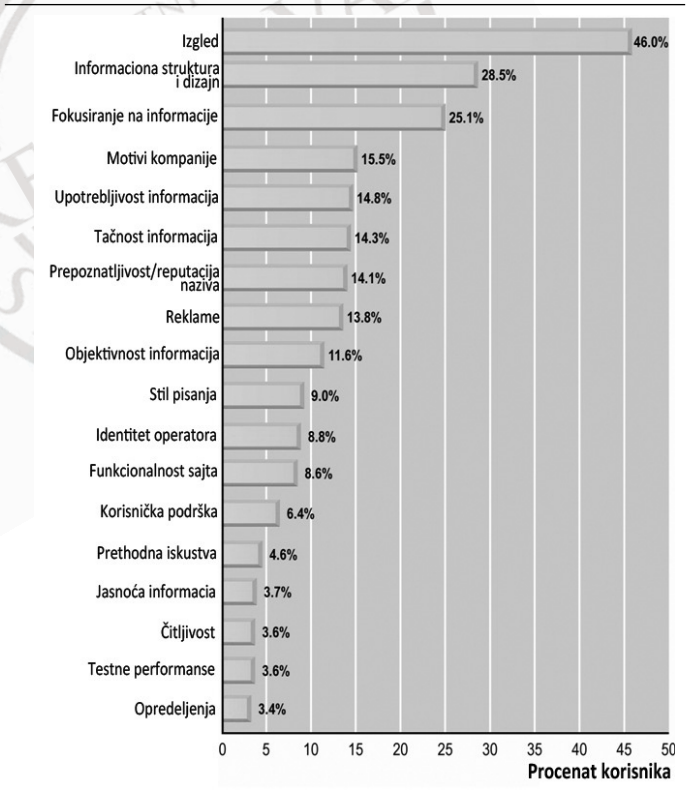
Faktori koji utiču na efektivnost softverskog interfejsa

- korisnost (funkcionalnost)
- lakoća korišćenja

Osim toga, za sajt e-trgovine je važno poverenje korisnika, koje se postiže:

- kvalitetom dizajna (gde spada i izgled sajta)
- dobrom navigacijom
- fokusiranje na informacije (razumljivošću, korektnim i aktuelnim sadržajem, odnosno informacionom strukturom)
- povezivanjem sa ostatkom Web-a
- bezbednošću podataka
- personalizacijom

Na Slici 8.11 su prikazani faktori e-trgovine po mišljenju korisnika [1], [4], [5].



Slika 8.11 Faktori kredibiliteta Web sajtova

Ilustracija: Invazivne tehnike marketinga

Invazivne tehnike marketinga su *Adware*, *Spyware*, reklamne bombe, marketing iz zasede i otimanje kupaca:

1. *Adware* je svaki računarski program koji prikazuje ili poziva neželjene reklame bez pristanka ili intervencije korisnika;
2. *Spyware* je svaki računarski program koji u toku rada prikuplja informacije o korisniku bez njegovog znanja;
3. *Reklamna bomba* (*Ad bomb*) je računarski program koji je tajno prenesen na računar klijenta sa namerom pozivanja neželjene reklame bez pristanka ili intervencije korisnika, kao što je npr. *Gator.com* (*Gain AdServer*), koji prikazuje reklame, a uz to prikuplja lične informacije (posećeni sajtovi, brojevi kreditnih kartica i slično). Reklame prikazuje i *Yahoo!Messanger*.
4. *Marketing iz zasede* (*Ambush marketing*) je besplatno korišćenje popularnosti različitih, pre svega sportskih događaja za svoju promociju. Vrši se promocija svojih proizvoda i usluga, tako što se vezuju za neku sportsku manifestaciju koristeći njenu popularnost i ugled, kao da kompanija zaista ima sponzorske ili neke druge veze sa poznatim i popularnim događajem.

   Suština ove tehnike je korišćenje velikih sportskih događaja u reklamne svrhe, bez plaćanja sponzorskih naknada organizatorima.

   Ova tehnika marketinga pojavila se usled velikog interesovanja za sponzorstvo, posebno u sportu. Osim neuspeha u dobijanju sponzorskih ugovora, razlog za primenu ove tehnike je izbegavanje velikih troškova sponzorstva na zaista velikim takmičenjima, kao što su olimpijade, svetska i evopska prvenstva.
5. *Otimanje kupaca* (*Customer hijacking*): koriste se samo-izvršni programi, preneseni na klijentske računare, koji omogućavaju kompaniji da otima kupce partnerskih markentiških sajtova i koji preusmeravju partnersku proviziju kidnaperu.

Invazivne tehnike marketinga na Web-u su u stalnom porastu.

8.4 LITERATURA

[1] Laudon K.C., Traver C.G., *E-commerce, business, technology, society*, 3rd Ed, Addison Wesley, 2006

[2] Symantec Corporation, *MessageLabs Intelligence: 2010 Annual Security Report*, 2011

[3] Symantec Corporation, *MessageLabs Intelligence: January 2011 Intelligence Report*, 2011

[4] Fogg, B.J., Soohoo, C., Danielson, D.R., Marable, L., Stanford, J., Tauber, E.R., *"How do users evaluate the credibility of Web sites? A study with over 2,500 participants",* Proceedings of DUX2003 Designing for User Experiences Conference, 2003.

[5] Stanford, J., Tauber, E.R., Fogg, B.J., Marable, L. , *"Experts vs. online consumers: A comparative credibility study of health and finance Web sites",* Consumer WebWatch Research Report, 2002. http://www.consumerwebwatch.org/pdfs/expert-vs-online-consumers.pdf

[6] www.marketingterms.com

[7] www.wikipedia.org

[8] www.google.com

[9] www.eroi.com

[10] www.smallbusiness.yahoo.com

9. BEZBEDNOST NA WEBU

9.1 UVOD

Elektronska trgovina se dominantno odvija na delu Interneta na kome se izvršava WWW servis. Stoga je neophodno upoznati praktičnu implementaciju servisa zaštite na ovoj infrastrukturi elektronskih transakcija. Kriptografski principi, koje smo upoznali u poglavlju 5 moraju se ugraditi u komunikacione protokole i softver, kao noseće elemente implementacije sistema zaštite. Na Internetu se koristi veliki broj protokola od kojih je svaki specijalizovan za svoj poseban zadatak. Neki od njih su namenjeni za obezbeđenje specijalnih komunikacionih servisa, kao što je na primer elektronska pošta ili pristup sistemu sa udaljenog terminala. Drugi su opšte namene i koriste se u različitim vidovima komuniciranja. Neki primeri protokola i njihovih implementacija mogu se videti u Tabeli 9.1.1

Protokol	Namena
CyberCash	Elektronsko slanje novca
DNSSEC	Imena domena
IPSec	Šifrovanje paketa podataka
PCT	Šifrovanje na nivou TCP/IP
PGP	Elektronska pošta
S/MIME	Elektronska pošta
S-HTTP	Web pretraživači
Secure RPC	Pozivi rutina sa udaljenog terminala
SET	Elektronsko slanje novca
SSL	Šifrovanje na nivou TCP/IP
SSH	Pristup sa udaljenog terminala
TLS	Šifrovanje na nivou TCP/IP

Tabela 9.1.1 Primer nekih važnijih Internet protokola i njihove namene

Dominantan protokol na Webu je SSL (Secure Socket Layer) [1]. Služi za šifrovanje komunikacija opšte namene između pretraživača (browser) i servera.

9.2 BEZBEDNOST NA STRANI KLIJENTA

Najveći potencijalni problem na Internetu je problem prisluškivanja na mreži. Postoje specijalni programi za ovu svrhu (packet sniffers). Ovakav program instaliran na spojnom putu između pretraživača i servera može da prikuplja sve vrste informacija, uključujući i sadržaj elektronskih formulara i informacije sadržane u specijalnim fajlovima (cookies). Protokol SSL značajno smanjuje rizik upotrebe Internet, štiteći podatke koji se prenose između pretraživača i servera i identifikujući svakog učesnika u vezi.

9.2.1 Pretraživači (browsers)

Microsoft Internet Explorer, Netscape Navigator i drugi komercijalni čitači-pretraživači koriste protokol SSL. Kada se pristupi zaštićenoj Web stranici, korisnički interfejsi ovih programa prikazuju indikatore koji obaveštavaju korisnika o tome. To su indikatori zaštićenog načina rada, indikatori nivoa bezbednosti itd. Takođe je i adresa takvih zaštićenih stranica drugačija, pošto sadrži ´s´ na kraju dela ´http´, tj. adresa počinje sa ´https´ umesto sa ´http´.

Pretraživači omogućavaju da se vide detalji o dokumentu kome se pristupilo, kao na primer metod šifrovanja, nivo bezbednosti (broj bita ključa), informacija o autentikacionim sertifikatima (pošiljaoca, primaoca, datum isteka sertifikata i izlazni niz iz hash funkcije sertifikata).

Primer: Kada se pristupi zaštićenoj Web stranici, Netscape Navigator prikazuje ikonicu katanca na ekranu. Njegova namena je da obavesti korisnika o tome da komunicira sa zaštićenom stranicom. Da bi dobio više informacija o zaštićenoj sesiji, korisnik može da izabere opciju iz menija View/Document Info. Ova opcija prikazuje informaciju o aktuelnom dokumentu. Najpre se prikazuje adresa aktuelne Web stranice. Zatim se daje informacija u vezi sa brojem bita ključa koji se koriste u aktuelnoj sesiji za šifrovanje informacija koje se prenose od pretraživača do servera. Na primer, ako se pretraživač nalazi van SAD, a server koji sadrži šifrovani dokument se nalazi u SAD, automatski se koristi 40 od mogućih 128 bita ključa za šifrovanje informacija. Posle informacije o dužini ključa, pojavljuje se informacija o sertifikatima: kome pripadaju, ko ih je izdao, broj serije, rok važenja i pripadajuća hash funkcija.

Microsoft Internet Explorer prikazuje korisniku informaciju o zaštićenoj Web stranici na sličan način kao i Netscape Navigator. Korisnik takođe može da dobije više informacija o dokumentu birajući opciju iz menija File/Properties/Security. Ova opcija prikazuje istu informaciju kao i Netscape Navigator, jedino postoji razlika u formatiranju.

Pošto su veze koje koriste protokol SSL značajno sporije od uobičajenih veza (bez šifrovanja), većina Web servera koristi normalni protokol http radi prikazivanja javnih Web stranica. Kada korisnik pokuša da pristupi zaštićenoj informaciji ili želi da pošalje šifrovanu informaciju (kao na primer podatke sa nekog on-line formulara), veza se prebacuje na URL https. U opštem slučaju, o tome korisnik ne mora da vodi računa, osim ako sam ne želi da vidi informaciju o zaštićenoj sesiji koristeći pomenute opcije iz menija svog pretraživača. Celokupna informacija koja se šalje preko on-line formulara, kao i informacija sadržana u cookie-ima, prenosi se u šifrovanom obliku.

Praktični problemi sa kojima se korisnik može suočiti prilikom upotrebe protokola SSL su sledeći:

1. Razlika između adrese koja se nalazi u sertifikatu i stvarne URL adrese servera. Kada pretraživač pristupi nekom SSL serveru, vrši osnovnu validaciju sertifikata tog servera. Ako je adresa koja se nalazi u sertifikatu različita od stvarne adrese URL, pretraživač upozorava korisnika. Zatim korisnik mora da odluči da li želi da pristupi toj Web stranici ili ne. U opštem slučaju, ako je razlika između pomenutih adresa velika, korisnik bi trebao da odustane od pristupa takvoj Web stranici.
2. Stranice sa mešanim sadržajem. Moguće je da HTML stranice sadrže mešavinu otvorene i šifrovane informacije. Na primer, glavna stranica može da bude šifrovana pomoću protokola SSL, dok slike na njoj mogu da dolaze sa drugog servera koji ne koristi šifru. U tom slučaju, pretraživač će posebno prikazati bezbednosnu informaciju za svaki element na stranici. Pretraživač se takođe može konfigurisati tako da obaveštava korisnika kada pristupi stranici sa mešanim sadržajem. Najgori slučaj je kada se pristupi nekoj Web stranici preko SSL, ali se sadržaj nekog formulara na toj stranici prenosi putem protokola koji ne koristi šifru. Ovaj slučaj je redak i može biti posledica greške autora Web stranice. Pretraživač može da detektuje ovakvu grešku i da obavesti korisnika da će se informacija prenositi u otvorenom obliku. Na žalost, mnogi korisnici isključuju ovu mogućnost i zbog toga ponekad prenesu informaciju u otvorenom obliku, iako to ne žele.
3. Upotreba kratkih ključeva, zbog ograničenja na dužine ključeva koje je uvela vlada SAD. Pretraživači namenjeni izvozu iz SAD i Kanade koriste ključeve dužine 40 bita. To nije dovoljno za zaštitu podataka, nezavisno od osobina algoritma za šifrovanje koji se koristi, zato što se prostor od 2^{40} ključeva može pretražiti u realnom vremenu. Neki korisnici van SAD koriste nadgradnje američkih pretraživača, namenjene za povećanje dužine ključeva (npr., program Safe Passage, itd.). Ove nadgradnje normalno funkcionišu kao proxy serveri. Na taj način, korisnik može da pošalje sve podatke u vezi sa URL takvom proxy serveru, koji ih šifruje koristeći ključ veće dužine i šalje šifrovane podatke udaljenom serveru.

4. Opoziv i isticanje roka važnosti sertifikata. U nekim slučajevima sertifikat nekog Web servera može biti opozvan. Na primer, može nastati štamparska greška u sertifikatu, ili privatni ključ može biti kompromitovan (tj. može ga saznati neko ko nije njegov legitimni vlasnik), u kom slučaju bi sertifikat mogao biti ilegalno korišćen. U svim pomenutim slučajevima, broj serije opozvanog sertifikata se stavlja na listu opozvanih sertifikata, koju održava ustanova za sertifikaciju. Na žalost, Web pretraživači ne proveravaju liste opozvanih sertifikata. Jedino u slučaju da sertifikatu istekne važnost, pretraživač će upozoriti korisnika, što će mu omogućiti da ne pristupi takvoj Web stranici.
5 Pristup Web stranici kojoj je sertifikat izdala ustanova nepoznata pretraživaču. Svaki Web pretraživač sadrži javne ključeve izdate od strane ustanova za sertifikaciju sa jednog spiska koji ima približno 35-40 članova. Ako korisnik pristupi Web stranici sertifikovanoj od strane ustanove koje nema u spisku unutar njegovog pretraživača, ponašanje pretraživača zavisi od programa koji se koristi. Na primer, Netscape Navigator upozorava korisnika i pita ga da li želi da prihvati takav sertifikat, u kom slučaju stavlja takvu ustanovu na svoju listu. Nasuprot tome, Microsoft Internet Explorer uvek prekida takvu sesiju, uz upozorenje korisniku da je nastupio takav događaj. Pretraživači takođe omogućavaju korisniku da instalira novu ustanovu za sertifikaciju. Sertifikati se distribuiraju putem Interneta ili na memorijskim medijumima. Posle instalacije takve ustanove za sertifikaciju, pretraživač će prepoznavati nove sertifikate i neće odbijati da pristupi takvim Web stranicama.

Web pretraživači su u stanju da prebacuju i izvršavaju softver automatski bez ikakvog obaveštavanja korisnika. Često korisnik ne zna da se izvršava neki program prebačen sa Weba na njegov računar. Ovakvo ponašanje pretraživača poznato je pod nazivom 'aktivni sadržaj' (active contents). Ako takav program sadrži u sebi grešku, pretraživač može da bude preopterećen, što dalje može da prouzrokuje opšti otkaz sistema. Ali takođe takav program može biti namerno napisan sa ciljem da se oštete datoteke u sistemu ili da se naruši poverljivost dokumenata. Nije lako razlučiti da li program sadrži slučajnu grešku ili namerno oštećuje elemente sistema. Na primer, kod složenih programa koji se često koriste verovatnoća nastajanja greške je visoka. Korisnik mora da aktuelizuje verziju takvog programa instaliranog na njegovom računaru da bi izbegao probleme koje prouzrokuju greške. Međutim, zlonamerna osoba može da modifikuje popularne programe i da ih prodaje na crnom tržištu po vrlo niskoj ceni. Zato je važno da se softver kupuje od prodavaca koji nude garancije.

Najčešće pretnje koje prouzrokuje softver su sledeće:

1. Trojanski konji – to su programi koje izvršava korisnik misleći da su korisni. Prilikom izvršenja mogu uneti virus u sistem, kopirati podatke u deo memorije kome autor takvog programa ima pristup kako bi otkrio tajne korisnika, ili prosto oštetiti sam sistem.

2. Virusi – to su mali programi koji su u stanju da se multiplikuju i da se ubacuju u izvršne programe, datoteke ili neke delove memorije. Kada se neki program zarazi virusom, on sam je u stanju da zarazi druge programe i datoteke. Virusi se prenose kroz sistem putem razmene datoteka.
3. Makro virusi – to su virusi napisani u makro jeziku nekog tekst procesora ili sličnog programa i rezidentni su unutar dokumenata koje takvi programi generišu. Zbog toga su u stanju da zaraze druge dokumente u bilo kom operativnom sistemu u kome se takav program izvršava.
4. Zečevi – to su programi koji su u stanju da naprave veliki broj kopija sebe samih, puneći memoriju računara u kome se izvršavaju i na taj način sprečavajući njegovo normalno funkcionisanje.
5. Crvi – to su programi slični zečevima, ali su u stanju i da se prenose sa jednog računara na drugi u mreži, koristeći slabosti komunikacionih protokola.

Virusi su najštetniji od svih gore pomenutih pretnji. Većina virusa nastaje modifikacijom već postojećih. Zbog toga je veoma važno koristiti antivirusne programe koji se redovno aktuelizuju.

Pretraživači često koriste eksterne programe radi otvaranja nekih dokumenata na Webu koje nisu u stanju sami da otvore. Postoje dva tipa takvih programa: pomoćne aplikacije (helper applications) i priključci (plug-ins). Pomoćne aplikacije su programi koji mogu da se izvršavaju nezavisno od pretraživača, dok se priključci mogu izvršavati jedino unutar pretraživača. Pretraživač Netscape koristi priključke, dok pretraživač Internet Explorer može da koristi takve priključke koje koristi Netscape, ali više koristi ActiveX komponente. Međutim, oba tipa aplikacija imaju jednu zajedničku osobinu: to su programi koji su u stanju da pristupe podacima u memoriji i drugim resursima korisnikovog računara. Zato greška u takvom programu ili jedan njegov deo namerno napisan od strane zlonamerne osobe može da ošteti sistem. Naročito su opasne takve aplikacije koje sadrže komandne interpretere, kao što su na primer COMMAND.COM, PERL, POWER-POINT, BASIC itd. Zbog toga je bolje koristiti komandne interpretere sa redukovanim mogućnostima, koji se pišu tako da su jedino u stanju da čitaju specifične dokumente. Čak i u tom slučaju, da bi se izbegli problemi usled slučajnih grešaka, poželjno ih je redovno aktuelizovati.

9.2.2 Java

Java je programski jezik koga je definisala kompanija Sun Microsystems radi korišćenja u tzv. uloženim sistemima (embedded systems) i kasnije adaptiran za korišćenje na Webu [2]. Njegova glavna prednost sastoji se u tome što koristi interpreter umesto programa prevodioca. Na taj način, program napisan u Javi može da se izvršava na svakoj kombinaciji hardvera i softvera na kojoj je instaliran Java interpreter. Kod drugih programskih jezika mora da se izvrši rekompilacija radi izvršavanja na različitom hardveru. Današnji

pretraživači (na primer, Netscape Communicator i Microsoft Internet Explorer) sadrže interpreter za Javu. Mnogi operativni sistemi takođe sadrže interne Java interpretere.

U stvarnosti, ono što se prenosi putem Interneta nije tekst programa napisanog u Javi (datoteka sa ekstenzijom .java). Na mestu nastanka, izvorna datoteka (.java) se prevodi čime se dobija jedna datoteka koja sadrži kompaktan kod (datoteka .class). Ova datoteka može da se komprimuje i memoriše u komprimovanoj formi, sa ekstenzijom .jar (Java archive). Java interpreteri instalirani na operativnim sistemima ili sadržani unutar pretraživača prepoznaju ovaj kod.

Programi napisani u Javi se izvršavaju na dva različita načina: način 'Application', koji je sličan normalnim programima napisanim u drugim programskim jezicima, i način 'Applet', kod koga se Java objekat prebacuje sa Web stranice i izvršava unutar pretraživača. Da bi se aplet smestio na HTML stranicu, potrebno je na nju smestiti jedan deo poznat pod imenom <APPLET> tag (oznaka). Ova oznaka sadrži informaciju o imenu apleta, adresi na kojoj se nalazi i dimenzijama prozora koje zauzima pri izvršenju. Takođe se može dodati i niz <PARAM> oznaka radi podešavanja ponašanja apleta za vreme izvršenja. Na sl. 9.2.1 prikazana je jedna <APPLET> oznaka.

```
<APPLET CODE="example_applet"
        CODEBASE="http://www.capricorn.org/java/"
        WIDTH=500 HEIGHT=100>
<PARAM NAME="image" VALUE="example.gif">
<PARAM NAME="color" VALUE="blue">
</APPLET>
```

Sl. 9.2.1 - Primer <APPLET> oznake unutar HTML dokumenta

Kada pretraživač pristupi <APPLET> oznaki, traži datoteku sa ekstenzijom .class ili .jar na naznačenoj adresi, startuje Java interpreter i izvršava aplet. Zatim aplet može da poziva druge datoteke .class koji su mu potrebni za izvršenje. Ove datoteke moraju da budu na istom serveru kao i sam aplet.

Aplet se u opštem slučaju pojavljuje u vidu novog prozora unutar prozora pretraživača. Može da izvršava animacije, da proizvodi zvukove i da odgovara na klikove miša i tastature. Takođe može da kreira svoje sopstvene prozore i menije. Prozori apleta su jasno označeni kao takvi, tj. drugačiji su od prozora operativnog sistema. Naslov takvog prozora je 'Untrusted Java window' ili 'Unsigned applet window', u zavisnosti od interpretera.

Bezbednosne implikacije izvršavanja Java aplikacija zavise od načina rada. Ako se radi u načinu 'Application', takav program ima sva prava i privilegije kao i svaki drugi program u operativnom sistemu. Može da čita i upisuje podatke u datoteke, šalje podatke na štampač, otvara linkove unutar mreže itd. Nasuprot tome, u načinu 'Applet' takav program ima mnoga ograničenja:

1. Aplet ne može da čita ni da upisuje podatke na lokalnom disku.
2. Aplet ne može da pristupi lokalnom hardveru, kao na primer fizičkoj memoriji, diskovima, kontrolerima tastature, štampača ili monitora.
3. Apleti ne mogu da pristupe informacijama o sistemskom okruženju, čak ni informaciji o operativnom sistemu koji se nalazi na računaru na kome se izvršavaju.
4. Apleti ne mogu da pozivaju sistemske komande ni da izvršavaju eksterne programe.
5. Apleti ne mogu da otvaraju mrežne linkove, osim veza sa računarom sa koga su prebačeni na mašinu na kojoj se izvršavaju (ovo ograničenje je poznato pod imenom phone-home ograničenje).

Zbog svega izloženog apleti ne mogu da pristupe niti da modifikuju privatne podatke sa računara na kome se izvršavaju. Ograničenje phone-home im omogućava da se povežu sa računarom sa koga su prebačeni na računar na kome se izvršavaju. Sa ovog računara apleti mogu da prebacuju podatke potrebne za izvršavanje.

Bezbednosni model Jave ostvaruje se kroz dve osobine Java interpretera.

Prvo, jedna specijalna klasa u Javi, poznata pod imenom 'Security Manager' upravlja svim pozivima koji mogu biti kritični sa stanovišta bezbednosti informacija. Ako jedan deo programa napisanog u Javi naruši bezbednosnu politiku apleta 'Security Manager' upozorava korisnika o tome i ne dozvoljava da se izvrši taj deo programa. Ovo upozorenje se naziva 'Security Exception'. Ako program sadrži grešku, poruka 'Security Exception' takođe može da se pojavi. To naravno ne znači da je takav softver napisan sa zlim namerama.

Drugo, Java interpreter sadrži jedan deo koji se naziva 'Bytecode Verifier', odgovaran za ispitivanje programa napisanih u Javi i proveravanje da li takvi programi poštuju ograničenja Java jezika za vreme prebacivanja sa izvora na računar na kome će se izvršavati. Ovaj verifikator služi za to da spreči da ekspert modifikuje Java aplet i tako izbegne izvršenje 'Security Managera'.

Iako je konstruisan imajući u vidu bezbednost informacija, Java aplet može da prouzrokuje probleme korisniku Web servisa. Radi se o sledećim problemima:

1. Teoretski, bezbednosni model Jave može da sadrži grešku. Neke greške su otkrivene i ispravljene u prvim verzijama interpretera, ali nema garancija da ne postoji još neka greška. Na primer, otkrivene su greške kod ograničenja phone-home, mogućnosti izvršenja bilo koje instrukcije mašinskog jezika, mogućnosti sprečavanja izvršenja 'Security Managera', itd. Zbog toga još uvek postoji mogućnost pojavljivanja opasnih apleta.
2. Moguće je napraviti aplet koji ulazi u beskonačnu petlju i na taj način značajno smanjuje resurse računara na kome se izvršava. Aplet takođe može da rezerviše jako veliku strukturu podataka u memoriji ili da napravi veliki broj sopstvenih kopija. Ako aplet otvori prozor koji je veći od prozora operativnog sistema, može

da spreči korisnika da pristupi prozorima ispod prozora apleta. Aplet takođe može da otvara nove prozore brže nego što korisnik može da ih zatvara. Pored toga aplet može da blokira pretraživač. To može biti rezultat greške, ali takođe može biti namerno prouzrokovano. Apleti koji se ponašaju na jedan od opisanih načina nazivaju se smetajućim apletima. Smetajući apleti se koriste prilikom napada na sistem poznate pod nazivom napadi radi odbijanja servisa.

3. Najvažniji problem u vezi sa Java apletima je sam bezbednosni model Jave, koji je tako restriktivan da ne dozvoljava konstrukciju praktično nijedne korisne aplikacije. Aplet ne može da pristupi nijednom resursu računara na kome se izvršava, čak ne može da izvršava ni elementarne zadatke kao što je štampanje, memorisanje informacija na disku, pretvaranje formata datoteka iz jednog u drugi i slanje datoteka putem. Zbog toga je originalni bezbednosni model Jave modifikovan tako da se neke restrikcije mogu ukinuti. Osnovno svojstvo novog bezbednosnog modela Jave je mogućnost potpisivanja koda apleta na način sličan sistemu Authenticode koji koriste komponente ActiveX. Apleti kojima su potrebne dodatne privilegije mogu se digitalno potpisati na način sličan onome koji koriste ustanove za sertifikaciju radi potpisivanja sertifikata servera. Ovaj sertifikat apleta može da pomogne korisniku da odluči da li da dozvoli izvršenje apleta na svom računaru ili ne.

9.2.3 ActiveX

Tehnologija ActiveX je razvijena na osnovu tehnologije OLE (Object Linking and Embedding) kompanije Microsoft [3]. Mali programi ActiveX poznati pod imenom 'komponente' (controls) mogu da urade sve što i Java apleti, uključujući kreiranje animacija, vizualizaciju multimedijalnih datoteka, upravljanje interakcijom sa mišem i tastaturom i kreiranje prozora. ActiveX komponente se smeštaju na HTML stranicu na sličan način onom na koji se smeštaju Java apleti. Primer smeštanja jedne ActiveX komponente na HTML stranicu može se videti na Sl.9.2.2

```
<OBJECT
    ID=”example_control”
    CLASSID=”clsid:7223B620-9FF9-11AF-00AA00C06662”
    CODEBASE=”http://www.capricorn.org/controls/”
    WIDTH=70 HEIGHT=40>
<PARAM NAME=”image” VALUE=”example.gif”>
<PARAM NAME=”color” VALUE=”blue”>
<PARAM NAME=”_version” VALUE=”3”>
</OBJECT>
```

Sl. 9.2.2 – Primer smeštanja ActiveX komponente na HTML stranicu

Oznaka <OBJECT> identifikuje komponentu po imenu, URL gde je smeštena i atribut CLASSID koji sadrži jedinstveni heksadecimalni broj komponente. Serijski broj omogućava da se komponenta automatski prebacuje sa unapred određenog servera (na primer, sa Microsoftovog). Parametri koji su potrebni komponenti za vreme izvršenja nalaze se u etiketi <PARAM>, na sličan način kao i kod Java apleta.

Najvažnija razlika između Java apleta i ActiveX komponenti je u tome što se ove druge prevode na mašinski jezik lokalnog računara. Komponente mogu biti napisane u bilo kom programskom jeziku (Delphi, Visual Basic, Visual C++ itd.) i prevedene u format pogodan za pristup iz memorije. Kada pretraživač pristupi oznaki <OBJECT>, prebacuje komponentu i poziva operativni sistem koji je smešta u memoriju i izvršava. To znači da ActiveX komponenta mora da se rekompiluje za svaku kombinaciju hardvera i softvera.

Iako ActiveX komponente imaju mnoge prednosti u odnosu na Java aplete (korišćenje svima poznatih programskih jezika u toku razvoja, mogućnost korišćenja postojećih programa prilikom razvoja komponenti, mogućnost izvršenja svega što programer želi), sa bezbednosne tačke gledišta predstavljaju veliku opasnost: pošto im je sve dozvoljeno na računaru na kome se izvršavaju, mogu takođe da kompromituju podatke ili da oštete sistem.

Imajući u vidu potencijalne pretnje prilikom upotrebe ActiveX komponenti, Microsoft zajedno sa kompanijom VeriSign digitalno potpisuje ActiveX komponente pomoću sistema koji se naziva 'Authenticode'. Digitalni potpis na jedinstven način identifikuje autora komponente i predstavlja solidnu garanciju da ta komponenta nije promenjena od trenutka potpisivanja. Kada pretraživač prebaci komponentu na lokalni računar, proverava validnost njenog digitalnog potpisa. Ako potpis ne postoji ili nije validan, ili ako je komponenta modifikovana, pretraživač je ne izvršava i upozorava korisnika o tome. U sistemu 'Authenticode' se koriste sertifikati koje obezbeđuje ustanova za sertifikaciju na način sličan onom koji se koristi kod sertifikacije Web servera. Pretraživači kao na primer Microsoft Internet Explorer i Netscape Communicator održavaju liste ustanova za sertifikaciju komponenti, kao i liste opoziva takvih sertifikata.

I pored svega navedenog, postoje potencijalni rizici upotrebe ActiveX komponenti. Sertifikati nisu jako skupi i svaka zlonamerna osoba može da ih pribavi. Zatim takva osoba može da razvije komponentu koja prouzrokuje štetu prilikom zadavanja neke neobične naredbe, a potom može reći da je takvo ponašanje komponente rezultat greške. Pored toga, iako sistem 'Authenticode' nudi korisniku mogućnost otkrivanja identiteta zlonamerne osobe posle nekog incidenta, on ne može da spreči da se takav incident dogodi. Zbog toga se ne preporučuje upotreba ActiveX komponenti u sistemima čiji su podaci važni sa stanovišta bezbednosti.

9.3 BEZBEDNOST NA STRANI SERVERA

Server povezan sa mrežom predstavlja elektronska vrata jedne organizacije. Zbog toga takođe predstavlja prirodnu metu za različite vrste napada. Neki napadači pokušavaju da izbegnu ograničenja servera, kako bi došli do dokumenata namenjenih samo za internu upotrebu. Drugi mogu da pokušaju da modifikuju sadržaj Web prezentacije radi izvrgavanja organizacije ruglu ili radi sprečavanja njenog normalnog funkcionisanja.

9.3.1 Osetljive tačke

Različiti su uzroci bezbednosnih problema sa Web serverima, ali u većini slučajeva radi se o sledećem:

1. Greške u sistemskom softveru – Greške u različitim delovima softvera se pojavljuju relativno često. Većina grešaka ne nastaje namerno, ali postoje greške koje mogu da posluže kao vrata kroz koja zlonamerna osoba može da se infiltrira u sistem i da dođe do informacija bez dozvole. Verovatnoća pojavljivanja greške raste sa povećanjem složenosti softvera. Posledice grešaka u softveru instaliranom na serveru nisu samo lokalnog karaktera. Takve greške utiču na sve računare koji su sa njim povezani. Tipične greške na Web serveru nastaju kada primi komandu koju autori softvera nisu dobro projektovali. Na primer, ako server obično prima komande koje nisu duže od 100 simbola, može početi da se neuobičajeno ponaša ako primi komandu dužine 10000 simbola. Napadači obično pokušavaju da iskoriste prisustvo grešaka u softveru radi infiltracije u sistem. Zbog međusobne konkurencije proizvođača softvera za servere, nove verzije softvera se pojavljuju često, pa se zbog toga one nikada u potpunosti ne ispitaju. Pored toga, moguće greške u softveru koji komunicira sa serverom takođe mogu da kompromituju bezbednost podataka na njemu.
2. Sistemski softver nije dobro konfigurisan – Čak i ako softver na Web serveru kao i sav softver u vezi sa njim ne sadrži greške, da bi server bio bezbedan potrebno je da drugi serveri u mreži, kao i operativni sistem budu dobro konfigurisani. Iako su operativni sistemi koji se koriste na Webu konstruisani na bezbedan način, u praksi da bi se realizovao ovaj cilj potrebno je podesiti mnoge parametre. U toku razvoja operativnog sistema on se konfiguriše sa parametrima koji obezbeđuju jednostavnu instalaciju. Na taj način se aktiviraju sve dozvole za vreme instalacije. Na primer, aktiviraju se popularni mrežni servisi, mogućnost konfigurisanja sa udaljenog terminala, a sistemske datoteke su veoma pristupačne. Korisnik čak ni ne zna koji tip servera (Web server, Gopher server, login server ili FTP server) je aktiviran neposredno posle instalacije. Ako korisnik sam ne konfiguriše server povećava se verovatnoća da on nije dobro konfigurisan.

Jedan od velikih problema u vezi sa konfiguracijom je problem pristupa datotekama. Višekorisnički operativni sistemi koriste privilegije svakog korisničkog računa da bi odredili mogućnost pristupa pojedinim resursima sistema. Postoji datoteka koja sadrži listu dozvola za svakog korisnika. Ako se ta lista konfiguriše tako da je korisnici mogu modifikovati, napadač može iskoristiti ovu mogućnost da bi povećao svoja prava i infiltrirao se u sistem sa privilegijama administratora. Mrežni servisi takođe imaju privilegije koje moraju da se ograniče na skup neophodan za dobro funkcionisanje. U suprotnom, mrežni server može biti meta napada na sistem višeg nivoa. Jednokorisnički operativni sistemi, koji nisu namenjeni za rad sa mrežnim serverima mogu postati meta napada sa odbijanjem servisa. Pored toga, kako ovakvi sistemi nemaju korisničke privilegije, svaka infiltracija u sistem omogućava napadaču pristup svim njegovim resursima.

3. Hardver servera nije bezbedan – Računar koji se koristi kao Web server ne bi smeo da se istovremeno koristi i kao računar opšte namene. Takođe treba voditi računa i o fizičkoj bezbednosti takvog računara.
4. Mreže nisu bezbedne – Svi podaci se preko Interneta prenose u otvorenom obliku, osim ako se ne izabere upotreba nekog kriptografskog protokola. Lozinke i korisnička imena predstavljaju osetljive tačke sistema, ako se prenose bez šifrovanja. Postoje specijalni programi poznati pod imenom 'password sniffers' koji mogu da obrade sve lozinke koje se prenose putem mreže. Ova tehnika se najčešće koristi za infiltraciju u sistem preko Interneta.
5. Administracija sistema sa udaljenog terminala nije bezbedna – Iako mogućnost pristupa sistemu sa administratorskim privilegijama sa udaljenog terminala predstavlja pogodnost za legalne administratore, ona takođe može olakšati upad u sistem potencijalnom napadaču. Zato se ne preporučuje česta upotreba ovog servisa.
6. Često se zaboravlja na pretnje koje potiču iz same organizacije ('insiders') – Mora se imati u vidu da postoje osobe koje su legalni korisnici sistema i koje zbog različitih razloga žele da zloupotrebe svoje privilegije (samo zbog radoznalosti ili zbog nekog ozbiljnijeg razloga). Organizacija takođe može da ima više od jednog Web servera. Može postojati javni server za korisnike Interneta, kao i nekoliko intranet servera za svako odeljenje unutar organizacije. Zato su intranet serveri osetljiviji na napade iznutra, dok su Internet serveri osetljiviji na napade spolja.
7. Ne vodi se računa o napadima sa odbijanjem servisa – Server može biti dobro konfigurisan, može se voditi računa o svim merama bezbednosti, ali ako je softver osetljiv na zadatke koji nisu unapred predviđeni, može doći do napada sa odbijanjem servisa. Primer ove situacije je greška pronađena u operativnim sistemima Windows NT i Windows 95 koji su za posledicu imali odbijanje servisa prilikom prijema specijalnog ping paketa.

8. Ne postoji politika bezbednosti – Ako ne postoji politika bezbednosti, ne može se znati da li je sistem bezbedan ili ne [4]. Politika bezbednosti mora da postoji u pisanom obliku i da sadrži listu pravila – šta sme da se radi u sistemu, a šta je zabranjeno za različite nivoe korisničkih prava. Politika bezbednosti takođe sadrži opise načina na koji se obavljaju različiti poslovi (pristup sistemu (login), administracja, backup, itd.).

9.3.2 Unix Web serveri

Operativni sistem Unix je dizajniran u vreme kada nisu postojali personalni računari [5]. Njegova osnovna karakteristika je da je to višekorisnički operativni sistem. To znači da jedan računar opslužuje velikom broju korisnika putem terminala. Svaki korisnik ima svoj direktorijum i lično okruženje i zaštićen je od uticaja drugih korisnika pomoću sistema dozvola pristupa. Datoteke, programi, hardverski i drugi resursi zaštićeni su kontrolom pristupa. Korisnik ne može pristupiti nijednom resursu ako za to ne dobije odgovarajuću dozvolu. Korisnici se grupišu prema zajedničkim privilegijama. Kada cela grupa dobije pravo pristupa određenom resursu, to pravo dobija i svaki njen član.

Svaki program koji se izvršava pod sistemom Unix, uključujući i one koji omogućavaju pristup servisima Interneta, poseduje privilegije korisnika sistema. Na primer, tipični sistem Unix sadrži korisnike ftp (ftp server), lp (server za upravljanje štampačima), itd.

Korisnik root (takođe se upotrebljava i naziv super korisnik (superuser)) je administrativni račun koji ima pristup svim resursima bez ograničenja. Ako neki servis dobije privilegije super korisnika, to može izazvati bezbednosne probleme. Zbog toga se ne preporučuje dodeljivanje svih privilegija servisu koji ima pristup Internetu.

Posle instalacije, sistem Unix je konfigurisan kao opšti sistem i njegova bezbednost mora da se poveća kako bi se koristio kao Web server. Povećanje bezbednosti obuhvata sledeće zadatke:

1. Instaliranje aktuelizacija ("patches") operativnog sistema.
2. Isključenje nepotrebnih servisa.
3. Definisanje minimalnog broja korisničkih računa.
4. Podešavanje dozvola pristupa datotekama i direktorijumima.

Preporučuje se izvršenje svih gore pomenutih operacija pre povezivanja računara sa mrežom.

Instaliranje aktuelizacija ("patches") operativnog sistema – Svaki program sadrži greške, a operativni sistemi nisu izuzetak u tom pogledu. Većina distributora operativnih sistema ima posebne Web adrese na kojima se mogu pronaći aktuelizacije tih sistema. Dobro je instalirati svaki "patch" u vezi sa bezbednošću. Pre instalacije, potrebno je napraviti backup sistema. Posle toga se instalira patch prema instrukcijama. U nekim slučajevima, instalacija patcha je laka, samo je potrebno kopirati novu verziju datoteke preko stare, ali u nekim slučajevima potrebna je rekompilacija jezgra operativnog sis-

tema. U opštem slučaju takođe je potrebno prekinuti vezu sistema sa mrežom za vreme instalacije patcha.

Isključenje nepotrebnih servisa – Posle instalacije, kod tipičnog Unix sistema uključeni su svi servisi. Na primer, posle instalacije sistema RedHat Linux, serveri FTP, Gopher, Web, mail, POP, NFS, pa čak i servis razmene datoteka sa sistemom Windows NT su uključeni, ali neki od ovih servera neće biti potrebni u aktuelnoj konfiguraciji. I ne samo to, neki od njih mogu predstavljati bezbednosne rizike ako se dobro ne konfigurišu.

Postoji dva tipa mrežnih servera u sistemu Unix. Serveri tipa "daemon" se uključuju za vreme inicijalizacije sistema. Server tipa daemon uvek je u funkciji i čeka zahtev od strane mreže. Obrađuje taj zahtev, a zatim čeka sledeći. Drugi tip servera nije stalno u funkciji, već se aktivira na zahtev programa inetd, koji je super daemon. Program inetd čeka zahtev od strane mreže, a zatim inicijalizuje specifičan server, koji obrađuje zahtev, a zatim se isključuje. Da bi se video listing Internet servisa koji su aktivni u Unix sistemu koristi se program netstat, koji lista sva ulazno-izlazna vrata sistema u stanju "listening". Serveri tipa daemon koji nisu potrebni isključuju se stavljajući komentare u odgovarajuće linije skript datoteka koje ih inicijalizuju. U novim sistemima, ove skript datoteke se obično nalaze na direktorijumu /etc/rc.d/init.d ili /sbin/init.d. Serveri tipa inetd koji nisu potrebni isključuju se stavljajući komentare u odgovarajuće linije datoteke /etc/inetd.conf. Posle ove operacije potrebno je restartovati sistem.

Definisanje minimalnog broja korisničkih računa – Većina napadača su osobe sa validnim korisničkim imenima i lozinkama. Ponekad oni dođu do validnih lozinki preko datoteke sa sistemskim lozinkama kojoj pristupaju koristeći neke greške u bezbednosnom sistemu. Drugi način na koji mogu doći do lozinki je automatska pretraga lozinki pomoću koje dolaze do loše odabranih lozinki (kao što su, na primer, reči koje imaju smisao, itd). Da bi se smanjila verovatnoća infiltracije u sistem preko lozinke dobijene na neki od opisanih načina, broj korisnika koji postoje u sistemu mora se redukovati u najvećoj mogućoj meri. Potreban je po jedan račun za svakog administratora sistema, ali autori Web stranica mogu da ih kreiraju na drugom računaru, a ne direktno na serveru. Posle toga se mogu prebaciti datoteke na server putem FTP servera.

Pored administratorskog računa (root), većina Unix sistema poseduje veliki broj računa za različite servere i daemone. Ponekad neki od ovih servera ima unapred dodeljene lozinke. Verovatnoća da potencijalni napadači poznaju ove predodređene lozinke je velika. Zbog toga je potrebno proveriti svaku liniju datoteke sa lozinkama /etc/passwd. Ako postoji takva lozinka, u odgovarajući deo linije se upiše zvezdica.

U opštem slučaju, dobra je praksa koristiti skript datoteke umesto manuelne izmene datoteke sa lozinkama, kad god se dodaju novi korisnici u sistem.

Podešavanje dozvola pristupa datotekama i direktorijumima – U većini slučajeva, neposredno posle instalacije pod operativnim sistemom Unix, svi korisnici mogu da pristupe svim direktorijumima i datotekama Web servera. Da bi se ovo sprečilo, moraju se modifikovati dozvole pristupa, da bi svaki pojedinačni korisnik imao pristup samo onom delu servera koji mu je potreban.

Postoje izvesni opšti tipovi direktorijuma koje koristi Web server, i to:

1. Konfiguracioni direktorijum – Ovaj direktorijum sadrži datoteke koji upravljaju operacijama na serveru. Te datoteke određuju sve operacije koje se odvijaju između vrata kroz koja server prima informacije iz mreže ("listens") i glavne stranice.
2. Datoteka alata Webmastera – Ova datoteka sadrži različite izvršne programe koje koristi Webmaster. To su alati za upravljanje pristupom serveru, za generisanje kriptografskih ključeva i za kreiranje indeksa dokumenata.
3. Direktorijum sa log datotekom – Ovaj direktorijum sadrži datoteke u koje se upisuju svi pristupi Web serveru, kao i sve greške koje se pojave za vreme rada servera.
4. Direktorijum CGI i direktorijum sa modulom servera – Direktorijum CGI sadrži skript datoteke koje se pozivaju prilikom kreiranja dinamičkih dokumenata, pristupa bazama podataka i izvršenja interaktivnih zadataka. Direktorijum modula servera sadrži module koje pišu korisnici radi povećanja mogućnosti servera.
5. Direktorijum sa dokumentima – Ovaj direktorijum je poznat pod imenom "document root". To je koren stabla koje sadrži HTML datoteke i sadrži datoteku sa dobrodošlicom servera i druge statičke dokumente.

Postoje takođe i neki opšti tipovi korisnika Web servera. Svaki od njih ima sopstvena bezbednosna pravila. Tipovi korisnika su sledeći:

- Webmaster – Webmaster je takođe poznat i pod imenom administrator servera. Potrebne su mu privilegije za čitanje i upisivanje na konfiguracioni direktorijum. Takođe mu je potrebna i privilegija za čitanje sa direktorijuma sa log datotekama.
- Web author – Ovom tipu korisnika potrebna je privilegija čitanja i upisivanja na direktorijum sa dokumentima.
- Web developer – Ovaj korisnik je Web author sa dodatnom privilegijom modifikacije CGI skript datoteka i modula servera.
- Web server – To je virtuelni korisnik kome je jedino potrebna privilegija čitanja stabla dokumenata i izvršenja CGI skript datoteka.

9.3.3 Kontrola pristupa

Većina Web servera omogućava svim korisnicima neograničen pristup celom stablu dokumenata. Međutim, kada je potrebno ograničiti pristup nekim dokumentima na serveru koristi se proces autentikacije korisnika. Ovaj proces služi za određivanje identiteta lica koje pristupa serveru. Posle autentikacije, proces autorizacije definiše resurse kojima korisnik može pristupiti.

Postoje različiti tipovi kontrole pristupa. U listi koja sledi, oni su dati po rastućem stepenu složenosti:

1. Kontrola pristupa zasnovana na IP adresi – Server proverava adresu korisnika i omogućava mu ili onemogućava pristup na osnovu te informacije. Svi Web serveri omogućavaju ovakav metod kontrole pristupa.
2. Kontrola pristupa zasnovana na imenu domena – Ovaj tip kontrole pristupa je sličan prethodnom. Jedina razlika je u tome što se ovde proverava ime domena umesto IP adrese. Kao i u prethodnom slučaju, svi Web serveri omogućavaju ovaj tip kontrole pristupa.
3. Kontrola pristupa zasnovana na korisničkom imenu i lozinci – Kod ovog tipa kontrole pristupa svaki korisnik dobija jedinstveno korisničko ime i sam bira svoju lozinku. Da bi pristupio delu servera sa ograničenim pristupom, korisnik mora da prezentuje korisničko ime i lozinku. Svi savremeni pretraživači i Web serveri omogućavaju ovaj tip kontrole pristupa.
4. Kontrola pristupa zasnovana na sertifikatima klijenata – Svaki korisnik sa udaljenog terminala dobija svoj kriptografski sertifikat koji se koristi kao digitalni potpis. Ovaj sertifikat izdaje ili treća strana od poverenja ili sama organizacija korisnika. Kada korisnikov pretraživač pokuša da se poveže sa Web serverom, on na zahtev servera prezentuje digitalni potpis korisnika. Ako je sertifikat validan i autorizovan, server omogućava pristup korisniku. Ovaj tip kontrole pristupa ne omogućavaju svi Web serveri, ali ga omogućavaju najnovije verzije najpopularnijih pretraživača (Netscape Communicator, Microsoft Internet Explorer).
5. Kontrola pristupa zasnovana na mrežnim bezbednosnim protokolima – Neki bezbednosni protokoli rešavaju generalni problem autentikacije i autorizacije u okviru LAN-a i WAN-a. Ti protokoli kao npr. Kerberos i DCE authentication mogu se koristiti kao softverski proizvodi za Web, ali samo specijalno konfigurisani pretraživači mogu da ih koriste. Zato su oni važniji za upotrebu u internim mrežama.

9.3.3.1 Osnovne tehnike (IP, ime domena, korisničko ime-lozinka)

Najjednostavniji tipovi kontrole pristupa zasnivaju se na imenu domena i/ili IP adresi udaljenog pretraživača. Pretraživači čije su adrese autorizovane mogu pristupiti serveru. Ovi tipovi kontrole pristupa mogu se koristiti radi omogućavanja selektivnog pristupa malom broju servera. Njihova prednost je u jednostavnosti i nemogućnosti nastajanja grešaka. Njihova najveća mana je nedostatak fleksibilnosti. Na primer, ako lokalni korisnik mora da promeni računar sa koga pristupa Web serveru, sa novog računara neće biti autentifikovan. Pristup se ne može ograničiti ni samo na jedan deo organizacije, naročito ako koristi proxy server.

Pomenuti tipovi kontrole pristupa osetljivi su na napad poznat pod imenom Domain Name Server (DNS) spoofing. Kod ovog napada, napadač privremeno preuzima kontrolu nad sistemom za pretraživanje imena servera. Zbog toga kasnije može da se predstavi kao legalni korisnik i da pristupi resursima servera. Da bi se smanjio rizik nastupanja ovakvog napada, može se koristiti firewall, ili dvostruka kontrola DNS, poznata pod imenom "paranoidna" kontrola. Na žalost, ove dodatne provere troše vreme CPU-a, pa ih korisnici često isključuju radi povećanja brzine rada.

Kontrola pristupa zasnovana na IP adresi udaljenog pretraživača je bezbednija i efikasnija od kontrole pristupa zasnovane na imenu servera. Međutim, osetljiva je na napad poznat pod imenom "IP spoofing", koji koristi jednu osobinu protokola TCP/IP koja se zove "source routing". U svakom slučaju, ovakav napad je redak, pošto ga nije lako sprovesti u praksi.

Mora se imati u vidu da pomenuti tipovi kontrole pristupa ne onemogućavaju fizičke napade na računare. To znači da ako napadači preuzmu fizičku kontrolu nad računarima sa legalnim imenima i IP adresama, mogu legalno pristupiti Web serveru.

Upotreba korisničkih imena i lozinki ima neke prednosti nad jednostavnom kontrolom zasnovanom na imenu servera i IP adresi. Te prednosti su sledeće:

1. Autentikuje se korisnik, a ne računar i zato je isključena mogućnost pristupa serveru čak i ako se preuzme fizička kontrola nad računarom.
2. Korisnici mogu da promene računare sa kojih pristupaju serveru.
3. Nema problema sa proxy serverima.
4. Većina korisnika prihvata ovaj tip kontrole pristupa, pošto im je ova tehnologija poznata.

Problemi koji se mogu pojaviti kod ovog tipa kontrole pristupa predstavljaju posledicu bezbednosne kulture korisnika (na primer, ako čuvaju lozinke u pisanom obliku, biraju loše lozinke, zaboravljaju lozinke, odaju lozinke svojim prijateljima, itd.). Takođe, većina implementacija ovog tipa kontrole pristupa prenosi lozinke bez šifrovanja.

9.3.3.2 Tehnike zasnovane na sertifikatima

Iako je upotreba lozinki jednostavna i efikasna, postoje problemi sa izborom, prisluškivanjem i odavanjem lozinki. Takođe, efikasnost ovog sistema se smanjuje ako se okruženje sastoji od velikog broja servera i hiljada korisnika. Rešenje problema u ovom slučaju nalazi se u upotrebi servera koji koriste SSL.

Sertifikate klijenata, takođe poznate i kao lične sertifikate, emituju ustanove za sertifikaciju. To mogu biti javne ustanove, čija je primarna uloga da emituju sertifikate, ili privatne ustanove u sastavu organizacije namenjene za sertifikaciju svojih zaposlenih. Iako javni sertifikati mogu da reše problem sertifikacije Internet servisa zasnovanih na prijavi (pretplati), kao i elektronske pošte, ne mogu da reše problem sertifikacije unutar jedne velike organizacije. Moguće rešenje ovog problema je da organizacija dobije

javni sertifikat, a zatim da sama organizacija izdaje sertifikat zaposlenom pri pristupanju i opozove ga pri napuštanju. Druga mogućnost je da sama organizacija postane ustanova za sertifikaciju.

Pored javnog ključa, sertifikat klijenta takođe sadrži i ime vlasnika, ime ustanove za sertifikaciju koja je izdala sertifikat, serijski broj i neke druge atribute. Ovi atributi sadrže različite podatke (tekstualne ili numeričke), kao što su adresa elektronske pošte, neposredni rukovodilac, profesionalna kategorija, odeljenje, broj kancelarije, broj telefona, datum rođenja, pol, broj lične karte, nacionalnost, itd. Atributi su fleksibilni u odnosu na pristup resursima sistema. Na taj način je moguće kontrolisati pristup bez održavanja velike baze podataka koja bi sadržala podatke o dozvolama pristupa.

Pouzdanost sertifikata klijenata određena je izvesnim faktorima kao što su kvalitet kriptografskog algoritma i privatnog ključa, procedura sertifikacije koju sprovodi ustanova za sertifikaciju, pouzdanost privatnog ključa korisnika, pouzdanost privatnog ključa ustanove za sertifikaciju, itd.

Problemi koji se mogu pojaviti prilikom upotrebe ličnih sertifikata su sledeći:

1. Korisnik zaboravlja lozinku koja se koristi za dešifrovanje njegovog privatnog ključa.
2. Korisnikov računar otkazuje prilikom promene korisničkog sertifikata ili privatnog ključa.
3. Korisnik aktuelizuje pretraživač i tom prilikom briše prethodno dobijene sertifikate.
4. Korisnik slučajno briše svoj sertifikat.
5. Korisnik ne zna koji od mogućih sertifikata koje poseduje treba da upotrebi da bi aktivirao servis koji mu je potreban.
6. Korisnikov privatni ključ je kompromitovan zbog nekog razloga (ukraden je njegov prenosni računar, itd.)

U većini pomenutih slučajeva, jedino rešenje je opoziv sertifikata. Ali opoziv sertifikata nije jednostavan proces, pošto se, na primer, mora održavati lista opozvanih sertifikata itd.

Kada pretraživač zahteva vezu sa Web serverom koji ima aktiviran protokol SSL v3.0 konfigurisan tako da od korisnika traži sertifikat, pretraživač mora da prezentuje sertifikat i da dokaže da je on legalan korisnik. Server proverava validnost sertifikata i prihvata ga ili odbija.

Posle prihvatanja sertifikata, server je spreman za izvršenje autorizacije i određivanja da li pomenuti korisnik može da pristupi resursu koji zahteva. Server može da testira autorizaciju jednostavnim proveravanjem informacije sadržane u sertifikatu, ili može da traži dodatnu informaciju sadržanu u internoj bazi podataka.

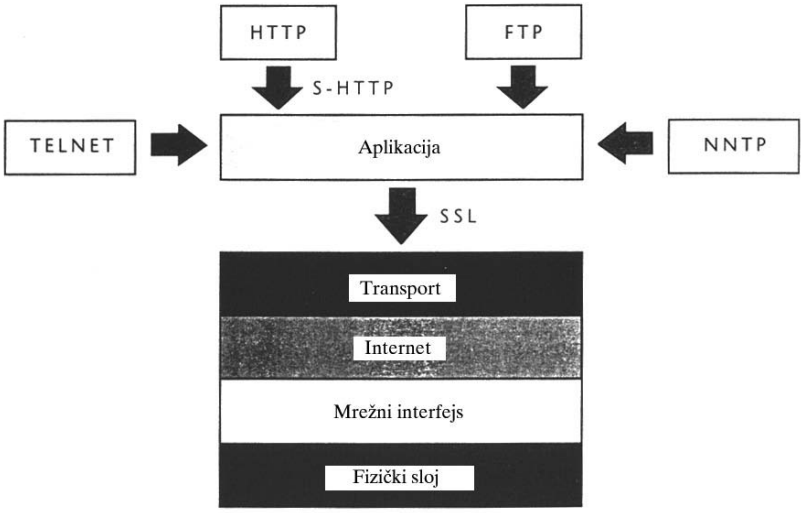
9.4 SECURE SOCKET LAYER (SSL)

Secure Socket Layer (SSL) je šifarski sistem opšte namene koji je uvela kompanija Netscape radi zaštite podataka na svojim pretraživačima. Posle verzije 3.0 ovog sistema, sve kompanije koje proizvode pretraživače su ga prihvatile i danas je implementiran u svim komercijalnim pretraživačima.

Protokol SSL se nalazi na transportnom nivou protokola TCP/IP, jedan nivo ispod nivoa aplikacija (kao na primer NTTP (news), HTTP (Web), SMTP (elektronska pošta) ili TELNET). Opšta šema protokola TCP/IP, na kojoj je prikazana pozicija SSL, prikazana je na Sl. 9.4.1.

Protokol SSL nije optimizovan samo za upotrebu unutar protokola HTTP i zato nije tako efikasan kao što bi bio kada bi bio konstruisan samo kao Web servis. Ovom protokolu je takođe potrebna veza posvećena samo protokolu TCP/IP. Kada se Web server izvršava u modu SSL, koristi vrata posvećena njegovim šifrovanim komunikacijama (obično se koriste vrata broj 443).

Protokol SSL je veoma fleksibilan, sa stanovišta izbora simetričnog algoritma šifrovanja, hash funkcije i metoda autentikacije. SSL može da koristi algoritam DES (u načinu rada CBC), trostruki DES, RC2 ili RC4 kao simetrične algoritme šifrovanja. Takođe može da koristi MD5 ili SHA kao hash funkcije. Radi autentikacije, SSL može da koristi algoritam RSA ili algoritam Diffie-Hellman za razmenu ključeva. Dužine ključeva mogu da variraju u zavisnosti od toga da li se algoritmi koriste unutar SAD ili van SAD. Skup koji se sastoji od simetričnog algoritma šifrovanja, hash funkcije i metoda autentikacije se naziva "cipher suite". U tabeli 1 prikazane su kombinacije koje sadrži SSL, verzija 3.0.



Sl. 9.4.1 – Pozicija protokola SSL unutar protokola TCP/IP

Na početku SSL veze klijenta sa serverom određuje se njihov zajednički cipher suite. U opštem slučaju, dve strane pokušavaju da pronađu najjači zajednički cipher suite. Na primer, ako pretraživač koristi jedino verzije sa 40 bita ključa i kontaktira sa serverom koji koristi ključeve veće dužine, u toj vezi će se koristiti ključevi dužine 40 bita. Na isti način, serveri iz SAD, iako su u stanju da koriste javne ključeve dužine 1024 bita, koristiće samo javne ključeve dužine 512 bita u vezama sa pretraživačima van SAD. Neki Web serveri omogućavaju administratorima da podešavaju parametre ovog procesa uspostavljanja veze. Na primer, moguće je dozvoliti pristup nekim delovima servera samo klijentima koji su u stanju da koriste ključeve veće dužine.

Protokol SSL takođe omogućava kompresiju podataka, koja se vrši pre šifrovanja. Za vreme SSL veze, celokupna komunikacija između pretraživača i servera u oba smera je šifrovana, uključujući i sledeće elemente:

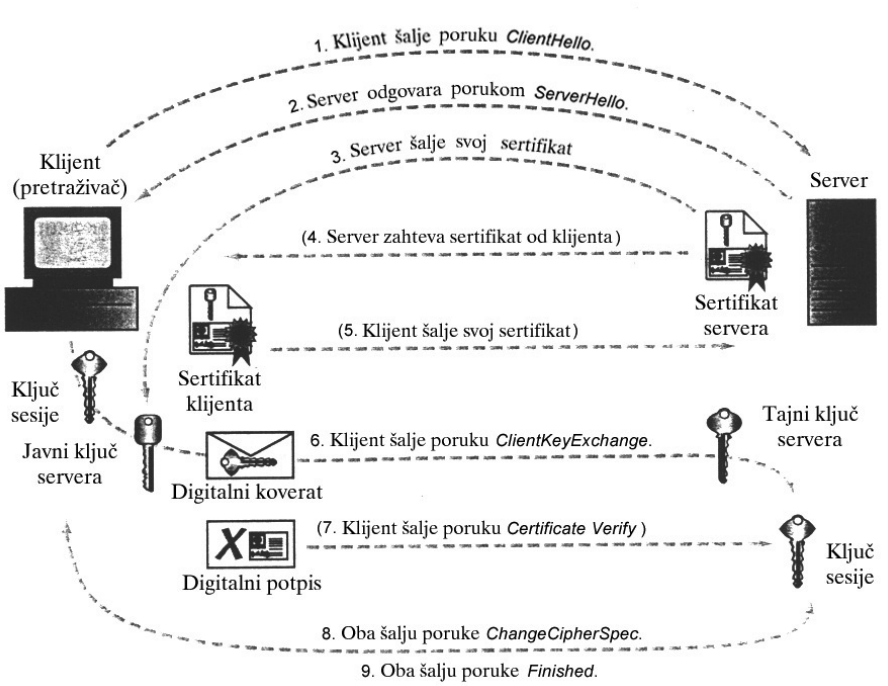
1. URL zahtevanog dokumenta.
2. Sadržaj zahtevanog dokumenta.
3. Sadržaji svih poslatih formulara.
4. "cookies" koje šalje pretraživač serveru.
5. "cookies" koje šalje server pretraživaču.
6. Sadržaj HTTP naslova.

Jedino što se ne može prikriti u SSL sesiji je činjenica da konkretan pretraživač komunicira sa konkretnim serverom. Da bi se ovo prikrilo, potrebno je koristiti specijalan proxy server.

Tabela 9.4.1 - Cipher suites u SSL

Suite	Nivo zaštite	Opis
DES-CBC3-MD5	Veoma visok	Triple DES u modu CBC, hash MD5, ključ dužine 168 bita.
DES-CBC3-SHA	Veoma visok	Triple DES u modu CBC, hash SHA, ključ dužine 168 bita.
RC4-MD5	Visok	RC4, hash MD5, ključ dužine 128 bita.
RC4-SHA	Visok	RC4, hash SHA, ključ dužine 128 bita.
RC2-CBC-MD5	Visok	RC2 u modu CBC, hash MD5, ključ dužine 128 bita.
DES-CBC-MD5	Srednji	DES u modu CBC, hash MD5, ključ dužine 56 bita.
DES-CBC-SHA	Srednji	DES u modu CBC, hash SHA, ključ dužine 56 bita.
EXP-DES-CBC-SHA	Nizak	DES u modu CBC, hash SHA, ključ dužine 40 bita.
EXP-RC4-MD5	Nizak	RC4 izvozna verzija, hash MD5, ključ dužine 40 bita.
EXP-RC2-CBC-MD5	Nizak	RC2 izvozna verzija u modu CBC, hash MD5, ključ dužine 40 bita.
NULL-MD5		Bez šifrovanja, hash MD5, samo autentikacija.
NULL-SHA		Bez šifrovanja, hash SHA, samo autentikacija.

Opšta šema protokola SSL prikazana je na Sl. 9.4.2 Namena ovog protokola je autentikacija servera i, opciono, klijenta i generisanje jednakog ključa na obe strane koji one mogu da koriste za šifrovanje svoje komunikacije.



Sl. 9.4.2 – Opšta šema protokola SSL

Koraci procedure su sledeći:

1. Klijent (tj., pretraživač) otvara vezu preko serverovih vrata i šalje poruku "ClientHello". Ova poruka sadrži sve kapacitete klijenta, uključujući verziju SSL sa kojom radi, cipher suites koje koristi i metode kompresije podataka koje je u stanju da koristi.
2. Server odgovara porukom "ServerHello". Ova poruka sadrži cipher suite i metod kompresije podataka koji je server izabrao, zajedno sa ID brojem sesije, koja je identifikuje. Na taj način, server je odgovoran za izbor cipher suite-a i metoda kompresije. Ako ne funkcioniše korespondencija između pretraživača i servera, server šalje poruku "Handshake failure" pretraživaču i prekida vezu.
3. Server šalje svoj sertifikat. Ako server koristi autentikaciju zasnovanu na sertifikatu (što je danas uobičajen slučaj), šalje svoj sertifikat u formatu X.509v3, digitalno potpisan.
4. Server može da zahteva sertifikat klijenta. Ova opcija ne koristi se često.

5. Klijent (opciono, na zahtev servera) šalje svoj sertifikat serveru. Ako klijent nema sertifikat, šalje upozorenje "No certificate" serveru. Po prijemu takvog upozorenja, server može da odbije vezu sa takvim klijentom.
6. Klijent šalje poruku "ClientKeyExchange". U ovom koraku bira se simetrični ključ. Detalji variraju u zavisnosti od izabranog cipher suite-a, ali u opštem slučaju klijent generiše tajni ključ koji se naziva "pre-master", koristeći generator slučajnih brojeva. Ovaj ključ se koristi na obe strane za generisanje pravog master ključa, kao ključa sesije. Pretraživač šifruje tajni ključ pomoću javnog RSA ključa servera (ovaj ključ se ekstrahuje iz sertifikata servera), radi kreiranja digitalnog koverta. Ovaj koverat se šalje serveru.
7. Klijent (opciono) šalje poruku "Certificate verify". Ova opcija se koristi ako klijent mora da se autentikuje serveru, što se čini proverom poznavanja privatnog RSA ključa.
8. Klijent i server šalju poruke "ChangeCipherSpec". To je jednostavna poruka koja potvrđuje da su obe strane spremne za početak komunikacije koristeći odabranu šifru i generisani ključ.
9. Klijent i server šalju poruke "finished". Ove poruke se sastoje od hash funkcija MD5 i SHA kompletne komunikacije do tog trenutka i omogućavaju da se obe strane uvere u to da su njihove poruke poslate bez modifikacije.

Počevši od tog momenta, obe strane počinju da komuniciraju šifrovano, koristeći ključ sesije za šifrovanje transakcija u oba smera.

Pored pomenutih koraka, verzija 3.0 protokola SSL sadrži i dodatnu transakciju u kojoj server šalje poruku "ServerKeyExchange". Ona se koristi za razmenu ključa sesije bez upotrebe sertifikata servera. Ovakav slučaj nastupa, na primer, kada se koristi protokol za anonimnu razmenu ključeva Diffie-Hellman [7]. Tada se klijent i server jedan drugom ne identifikuju.

9.5 LITERATURA

[1] SSL 3.0 specification, at http://wp.netscape.com/eng/ssl3/

[2] http://www.java.com/en/

[3] http://www.active-x.com/

[4] M.Milosavljević, G.Grubor, "Osnove bezbednosti i zaštite informacionih sistema", Univerzitet Singidunum, Beograd, 2006.

[5] http://www.unix.org/

[6] http://en.wikipedia.org/wiki/Windows_NT

[7] M.Stamp, "Information Security – Principles and Practice", John Wiley & Sons, Wiley-Interscience, 2006.

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

10. USTANOVE ZA SERIFIKACIJU I DIGITALNI SERTIFIKATI

Kriptografija sa javnim ključevima dobro funkcioniše ako pošiljalac unapred poznaje identitet primaoca. To nije uvek lako osigurati. Imajući u vidu stotine hiljada Web servera i milione potencijalnih klijenata, nije moguće uskladištiti javne ključeve svih korisnika u memoriji jednog klijenta (na primer, na disku). Takođe, nije moguće zahtevati javni ključ svakog recipienta pre slanja šifrovane poruke, pošto nema garancije da je recipient upravo onaj za koga se predstavlja.

Jedno rešenje ovog problema bilo bi održavati veliku bazu podataka sa svim javnim ključevima, iz koje bi se distribuirali javni ključevi na zahtev klijenta. Ali u tom slučaju bi se pojavili drugi problemi, kao na primer problem efikasnosti sistema sa tolikim brojem korisnika i tako velikom bazom.

10.1 POTREBA ZA USTANOVAMA ZA SERTIFIKACIJU

Jedno praktičnije rešenje pomenutog problema je verovati trećoj strani, poznatoj kao "ustanova za sertifikaciju", [1], [2], [3]. Ovakve ustanove verifikuju javne ključeve. Ustanova za sertifikaciju je preduzeće koje skladišti informacije o identitetu fizičkih i pravnih lica. Umesto držanja svih javnih ključeva u memoriji korisnika, on skladišti samo javne ključeve malog broja ustanova za sertifikaciju. Pre slanja poruke nekome, pošiljalac zahteva od primaoca digitalni sertifikat potpisan od strane pomenutih ustanova za sertifikaciju. Na taj način pošiljalac može da proveri identitet primaoca i da ekstrahuje iz sertifikata njegov javni ključ.

10.2 ELEMENTI DIGITALNOG SERTIFIKATA

Osnovni elementi svakog digitalnog sertifikata su sledeći:

1. Informacija o identitetu vlasnika (subjekta) – Sadrži ime, prezime(na), adresu elektronske pošte, broj telefona, fizičku adresu, itd.
2. Javni ključ vlasnika.
3. Naziv ustanove za sertifikaciju.
4. Digitalni potpis ustanove za sertifikaciju.

Pored pomenutih elemenata, sertifikati sadrže i dodatne informacije, kao na primer verziju sertifikata, serijski broj, rok važenja, itd.

10.3 POLITIKE SERTIFIKACIJE

Digitalni sertifikati se konstruišu tako da se ne mogu falsifikovati sa realnim računarskim resursima. Sistem funkcioniše na sledeći način:

1. Klijent generiše par javni ključ – tajni ključ.
2. Tajni ključ se memoriše, a javni ključ se šalje ustanovi za sertifikaciju, zajedno sa informacijom o identitetu, u obliku "zahteva za sertifikaciju ".
3. Ustanova za sertifikaciju proverava identitet pošiljaoca.
4. Ako je sve u redu, ustanova za sertifikaciju kreira sertifikat, koji sadrži javni ključ klijenta, kao i informaciju o njegovom identitetu. Ako se ovaj sertifikat koristi unutar pretraživača, može da sadrži i ime i adresu elektronske pošte klijenta. Sertifikat koji će se koristiti na Web serveru sadrži njegov URL.
5. Ustanova za sertifikaciju izračunava vrednost hash funkcije sertifikata i potpisuje je svojim tajnim ključem, kreirajući na taj način potpisani sertifikat. Zatim šalje takav sertifikat klijentu.

Ustanove za sertifikaciju i potpisani sertifikati su osnovne komponente sistema za distribuciju ključeva poznatog pod imenom "infrastruktura javnih ključeva". Različiti tipovi sertifikata imaju različite namene. Na primer, sertifikati koji se koriste za autentikaciju Web servera nazivaju se sertifikatima servera. Oni koji autentikuju individualne korisnike nazivaju se personalnim sertifikatima. Oni koje upotrebljavaju proizvođači softvera radi potpisivanja izvršnih datoteka nazivaju se sertifikatima proizvođača softvera. Naravno, postoje i sertifikati koji sadrže javne ključeve ustanova za sertifikaciju koji se nazivaju sertifikatima ustanova za sertifikaciju. Iako imaju različite namene, svi sertifikati imaju isti format, poznat kao X.509v3 (verzija 3 formata X.509) [4].

Politika sertifikacije je imenovani skup pravila koja regulišu mogućnosti dodeljivanja sertifikata određenoj organizaciji i/ili aplikaciji sa karakterističnim bezbednosnim zahtevima. Na primer, jedna politika sertifikacije bi mogla da reguliše mogućnost dodeljivanja sertifikata radi autentikacije EDI transakcija u određenom opsegu cena. Ustanova za sertifikaciju, kao i svi korisnici moraju da prihvate politiku sertifikacije.

U nastavku se daje primer jedne politike sertifikacije:

Finansijska politika preduzeća XYZ – Ova politika se koristi radi zaštite finansijskih transakcija čija vrednost je veća od 2000 eura. Parovi sertifikovanih ključeva moraju da se generišu i skladište u hardveru. Element hardvera koji sadrži takve ključeve dodeljuje se jedino rukovodstvu preduzeća i licima sa posebnog spiska. Da bi autorizovanom licu bio dodeljen takav element hardvera, ono mora da se lično pojavi u odeljenju za bezbednost i da pokaže ličnu kartu.

Iako ne postoje standardni elementi koje mora da sadrži politika sertifikacije, mogu se kao neophodni nabrojati sledeći:

1. Ograničenja u vezi sa licima i primenljivošću – Ustanova za sertifikaciju može da dodeljuje sertifikate samo članovima određene organizacije, na primer zaposlenima. Osim toga, sertifikati koji pripadaju konkretnoj politici mogu služiti jedino za specifične namene.
2. Politika identifikacije i autentikacije – To je praksa koju primenjuje ustanova za sertifikaciju za vreme procesa identifikacije i autentikacije vlasnika sertifikata.
3. Politika zaštite ključeva – To su mere koje sprovodi ustanova za sertifikaciju radi zaštite svojih sopstvenih ključeva i ključeva svojih klijenata.
4. Operativna politika – To je praksa koju sprovodi ustanova za sertifikaciju za vreme rada njenih servisa, na primer, frekvencija kojom emituje liste opozvanih sertifikata.
5. Lokalna bezbednosna politika – To su mere koje sprovodi ustanova za sertifikaciju, kao i njeni klijenti radi obezbeđenja svog neposrednog okruženja. Tu spadaju fizičke mere zaštite, lična bezbednost itd.

10.4 DIGITALNI SERTIFIKATI JAVNIH KLJUČEVA

Najvažnija vrsta sertifikata je sertifikat javnog ključa u kome se vrednost javnog ključa entiteta dodeljuje skupu njegovih personalnih podataka. Ovaj sertifikat se digitalno potpisuje od strane ustanove za sertifikaciju. Kada pošiljalac želi da šifruje poruku koristeći tehnologiju sa javnim ključevima, potrebna mu je kopija javnog ključa primaoca. Pošiljalac mora da bude siguran da je javni ključ primaoca koji poseduje originalan. U protivnom bi sadržaj tajnog dokumenta, iako šifrovan, bio otkriven napadaču koji se predstavlja kao legalni primalac.

Sertifikat javnog ključa koji se najviše koristi ima jedinstven format, definisan standardom ISO/IEC/ITU X.509.

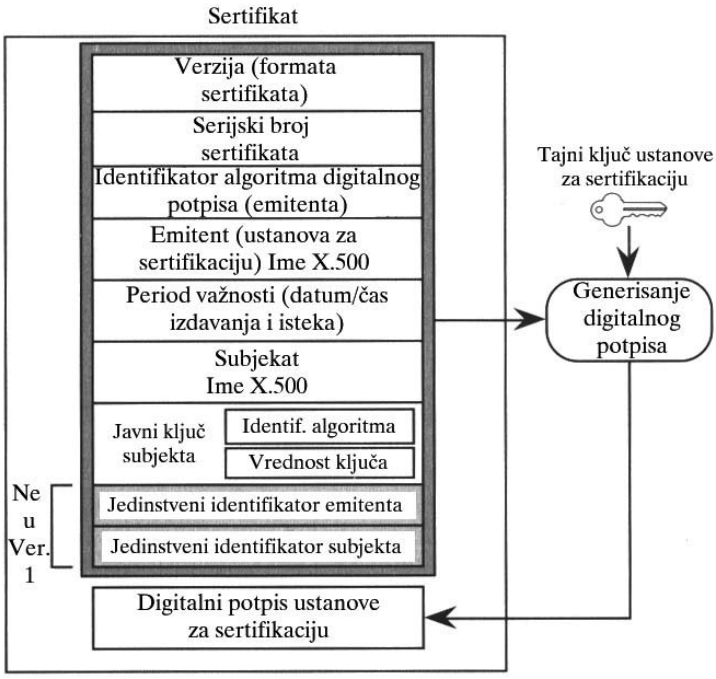
10.4.1 Standard X.509

Postoje tri verzije formata sertifikata X.509: prva, izdata 1988. godine, druga, izdata 1993. godine i treća, izdata 1996. godine. Svaka verzija osim prve sadrži sve rubrike prethodne verzije uz nove dodatne rubrike. Osnovni elementi ovog standarda prikazani su na Sl. 10.4.1.

10.4.2 Rubrike i sadržaj sertifikata

Rubrike sertifikata su sledeće:

1. Verzija – To je indikator verzije standarda (1, 2 ili 3), sa mogućnošću dodavanja narednih verzija.



Sl. 10.4.1 – Format sertifikata X.509, verzija 1 i 2

2. Serijski broj – To je jedinstveni broj sertifikata, koji mu pridružuje ustanova za sertifikaciju koja ga izdaje.
3. Tip digitalnog potpisa – Sadrži identifikaciju digitalnog potpisa, koji koristi ustanova za sertifikaciju.
4. Ustanova za sertifikaciju – Sadrži ime ustanove za sertifikaciju u formi definisanoj standardom X.500. Ovaj standard definiše specijalno stablo imena ustanova za sertifikaciju (struktura direktorijuma). Na taj način se definiše lanac sertifikacije, počevši od glavne ustanove (na primer, vlade) do ustanove neposredno iznad nivoa klijenta, koja izdaje konkretan sertifikat.
5. Rok važenja – Sadrži datum izdavanja i datum isteka važnosti sertifikata.
6. Subjekt – To je ime vlasnika sertifikata u formi definisanoj standardom X.500.
7. Informacija o javnom ključu subjekta – Sadrži vrednost javnog ključa subjekta, zajedno sa identifikacijom algoritma šifrovanja u kome će se koristiti.
8. Jedinstvena identifikacija ustanove za sertifikaciju (opciono) – Ovo polje može da sadrži dodatnu informaciju o identitetu ustanove za sertifikaciju. Ako postoji više od jedne ustanove za sertifikaciju sa istim imenom, takva informacija je neophodna.
9. Jedinstvena identifikacija subjekta – Ovo polje može da sadrži dodatnu informaciju o identitetu subjekta. Ako postoji više od jednog subjekta sa istim imenom, ova informacija je neophodna.

10.4.3 Ekstenzije (X.509v3)

Za vreme važenja verzija 1 i 2 standarda X.509, korisnici su osetili potrebu za dodavanjem dodatnih polja. Razlozi za definisanje nove verzije su bili sledeći:

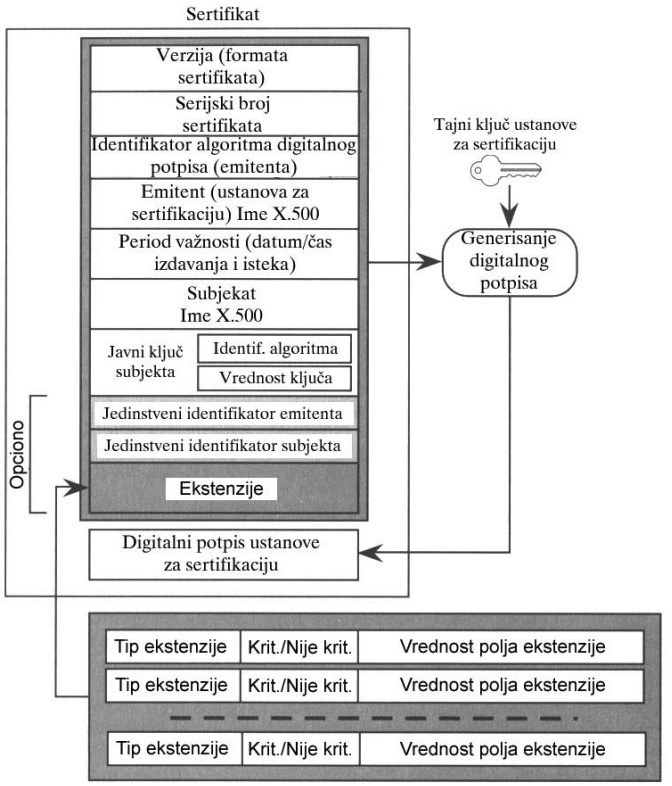
1. Subjekti mogu da imaju više od jednog sertifikata sa različitim javnim ključevima koji se koriste za različite servise. Pored toga, parovi tajni ključ – javni ključ moraju redovno da se zamenjuju novim.
2. Potrebno je više informacija o imenima (ustanove za sertifikaciju i subjekta) nego što nudi standard X.500.
3. Nekim aplikacijama (servisima) potrebna je sopstvena forma prezentacije imena, različita od standarda X.500. Primer takve aplikacije je elektronska pošta.
4. Različiti sertifikati mogu biti izdati u skladu sa različitim politikama sertifikacije.
5. Potrebno je smanjiti složenost prezentacije lanca sertifikacije. Na primer, kada jedna ustanova za sertifikaciju izda sertifikat drugoj ustanovi za sertifikaciju, potrebna joj je jedino informacija o skupu sertifikata koji je ona emitovala do nižeg nivoa (na primer, sertifikati koji pripadaju jednom skupu imena).

Nova verzija standarda pojavila se 1996. Njena šema je prikazana na Sl. 10.4.2.

Razlika između verzije 3 i prethodnih verzija standarda X.509 je u tome što nova verzija poseduje dodatna polja (ekstenzije). Ove ekstenzije omogućavaju dodavanje proizvoljnog broja polja.

Svako polje ekstenzije ima svoj sopstveni tip koji je potrebno registrovati, tj. pridružiti mu identifikaciju objekta. Na taj način, bilo ko može da definiše tip ekstenzije. Međutim, tipovi koji se najčešće koriste su standardizovani. Ovi tipovi se nazivaju standardnim ekstenzijama sertifikata.

Svako polje ekstenzije takođe sadrži i karakterizaciju kritičnosti "critical" ili "non-critical". Ako je vrednost te karakterizacije "non-critical", sistem koji koristi sertifikat može da ignoriše ovo polje ukoliko ga ne prepoznaje. U suprotnom, tj. kada sistem ne prepoznaje ovaj tip ekstenzije, preporučuje se da se ne koristi nijedan deo sertifikata.



Sl. 10.4.2 – Šema sertifikata prema standardu X.509v3

Treći deo ekstenzije je vrednost ekstenzije. Tip vrednosti (string, datum ili neki složeniji tip) zavisi od tipa ekstenzije.

Standardne ekstenzije sertifikata su uključene standard X.509v3 1997. godine. Podeljene su u sledeće grupe:

1. Informacije o ključu i politici sertifikacije.
2. Atributi subjekta i ustanove za sertifikaciju.
3. Ograničenja lanca sertifikacije.
4. Ekstenzije u vezi sa listama opoziva sertifikata.

10.5 OPOZIV SERTIFIKATA

Sertifikat javnog ključa ima ograničen rok važnosti, koji se nalazi u odgovarajućem polju. Rok važnosti jednog sertifikata zavisi od politike sertifikacije koju sprovodi ustanova za sertifikaciju. U opštem slučaju, rok važnosti sertifikata se nalazi u opsegu od nekoliko meseci do nekoliko godina.

Počevši od datuma početka važnosti sertifikata, pretpostavlja se da će on važiti do datuma isteka. Ali ponekad, zbog različitih uzroka, potrebno je prekinuti važnost sertifikata pre ovog roka. Neki od uzroka su sledeći: dekonspiracija tajnog ključa, promena imena subjekta, promena odnosa između subjekta i ustanove za sertifikaciju, itd. U takvim slučajevima, ustanova za sertifikaciju može da opozove sertifikat.

Ustanova za sertifikaciju je odgovorna za donošenje odluke o opozivu sertifikata. Ova akcija se obično sprovodi na zahtev ovlašćenog lica. Ovlašćeno lice za opoziv sertifikata mora da bude poznato svim korisnicima. U opštem slučaju, korisnik ima pravo da zahteva opoziv svog sertifikata. Službenici ustanove za sertifikaciju su takođe ovlašćeni da opozovu sertifikate, pod unapred određenim uslovima koji su poznati svim korisnicima. Pored toga, i druga lica mogu steći pravo da zahtevaju opoziv sertifikata, na primer. korisnikov neposredni rukovodilac, itd.

Ustanova za sertifikaciju mora da autentikuje svaki zahtev za opoziv sertifikata. Kada donese odluku o opozivu sertifikata, ustanova za sertifikaciju informiše sve korisnike o tom događaju. Način na koji se ovo sprovodi u praksi je periodičnim objavljivanjem specijalnog izveštaja, poznatog pod imenom lista opozvanih sertifikata (Certification Revocation List - CRL). Pojam CRL je opisan u standardu X.509. CRL je lista opozvanih sertifikata, koju digitalno potpisuje ustanova za sertifikaciju. Ova lista se objavljuje i njoj imaju pristup svi korisnici. Može se nalaziti, na primer, na jednom unapred određenom Web serveru. Svaki opozvani sertifikat se unutar CRL identifikuje po svom serijskom broju.

Pre korišćenja sertifikovanog javnog ključa, sistem mora da verifikuje da se sertifikat ne nalazi na CRL. Naravno, CRL mora da se redovno ažurira. Pojam ažuriranja CRL nije definisan na precizan način i nije standardizovan. Ažuriranje zavisi od lokalne politike sertifikacije. Ali, prema većini politika sertifikacije, ažuriranje znači da se koristi poslednja verzija CRL.

Ustanova za sertifikaciju objavljuje CRL na kraju perioda određenog aktuelnom politikom sertifikacije. Nova CRL se objavljuje u tom trenutku čak i ako ne postoji razlika između aktuelne i prethodne CRL. CRL se takođe mogu objavljivati i na drugi način, kao na primer, korišćenjem sigurnih kanala, itd.

Veličina CRL je veoma važna zato što svaki korisnik mora da proveri CRL pre početka korišćenja javnog ključa. Zbog toga se elementi CRL brišu posle isteka odgovarajućeg roka važnosti. U verziji 3 standarda X.509, dozvoljava se da se skup korisnika podeli i da se definiše više od jedne CRL. Na taj način, svaka od CRL može da se nalazi na posebnom serveru (na primer, Web serveru). Tako ustanova za sertifikaciju može da kontroliše veličinu svake CRL. Na primer, CRL može da se podeli prema razlozima opoziva itd.

U slučaju konflikta između ustanove za sertifikaciju i vlasnika sertifikata, sertifikat se može privremeno suspendovati, bez opoziva, do razrešenja konflikta. U tom slučaju, prema dodatnom standardu ANSI X9, definiše se "hold" status sertifikata. Kasnije se status "hold" može pretvoriti u status "revoked" ili se sertifikat može ukloniti sa CRL.

10.6 NEPORECIVOST

Svi pojmovi i servisi definisani do ovog trenutka predstavljaju okruženje elektronske trgovine. Pored bezbednosnih servisa na Web-u, potrebno je definisati i algoritme za implementaciju neporecivosti. Potom se može preći na opisivanje specifičnih servisa koji ostvaruju transakcije novca putem digitalnih mreža, posebno putem Interneta. Neporecivost se može definisati kao atribut komunikacije koji je štiti od situacije da jedna od strana učesnica negira da je do komunikacije došlo. Način implementacije servisa neporecivosti zavisi od korišćenih protokola i mehanizama, kao i od servisa koje obezbeđuje treća strana.

10.6.1 Pojam neporecivosti

U praksi se termin "neporecivost" počeo koristiti osamdesetih godina. 1988. godine je ISO uveo standard bezbednosne arhitekture u otvorenim sistemima. Od tada se ovaj termin koristi u mnogim međunarodnim standardima. U tim standardima, nporecivost se opisuje kao bezbednosni servis uperen protiv negacije jedne od strana učesnica u komunikaciji da je učestvovala u njoj. Postoji takođe i pravna definicija porecivosti.

Ovde se neporecivost tretira kao servis u kome se definiše koji tip informacije je potreban da bi se razrešili konflikti koji mogu da nastanu posle neke komunikacije.

Svaka komunikacija, bilateralna ili multilateralna, obuhvata dve osnovne vrste učesnika – pošiljaoce i primaoce. Tako se neporecivost može podeliti na dva dela: neporecivost porekla i neporecivost prijema. Dodatni poseban slučaj je neporecivost slanja, tj.

sposobnost sprečavanja ili razrešavanja konflikata kod kojih jedna od strana negira da je poslala konkretnu poruku na konkretnu adresu.

Neporecivost porekla sprečava ili razrešava konflikte kod kojih jedna odstrana negira da je bila izvor konkretne poruke, ili negira tačno vreme konkretne transakcije ili obe stvari.

Da bi se u praksi sprovela neporecivost u ovom slučaju, primaocu je potrebna sledeća informacija:

1. Identitet pošiljaoca.
2. Sadržaj poruke koju je poslao pošiljalac.
3. Datum i čas komunikacije.
4. Identiteti svih primalaca koji su primili istu poruku.
5. Identiteti svih trećih strana od poverenja, uključenih u generisanje evidencionih dokumenata ("documents of evidence").

Primaocu je potrebna bar informacija sadržana u tačkama 1 i 2 iz gornje liste.

Neporecivost prijema sprečava ili razrešava konflikte kod kojih jedna strana negira da je primila konkretnu poruku, ili negira da je primila tu poruku u konkretnom trenutku, ili negira obe stvari.

Da bi se u praksi ostvarila neporecivost u ovom slučaju, pošiljaocu je potrebna sledeća informacija:

1. Identitet primaoca.
2. Sadržaj poruke.
3. Datum i čas prijema poruke.
4. Identitet svih trećih strana od poverenja uključenih u generisanje evidencionih dokumenata.

Neporecivost slanja sprečava ili razrešava konflikte sa sledećim karakteristikama:

1. Pošiljalac tvrdi da je poslao poruku, ali primalac ne samo što tvrdi da nije primio poruku, već takođe tvrdi da pošiljalac nije ni poslao poruku.
2. Pošiljalac tvrdi da je poslao konkretnu poruku konkretnog datuma i konkretnog časa, ali primalac tvrdi da ta poruka nije poslata ni tog datuma ni tog časa.

Ako i pošiljalac i primalac govore istinu, moguće je da je nastupila greška u komunikacionom sistemu.

Neporecivost slanja je posebno korisna u slučajevima kada su datum i čas slanja značajni. Očigledno je da je neporecivost slanja jedna varijanta neporecivosti prijema (oba servisa štite pošiljaoca, metodi implementacije su slični, itd.).

10.6.2 Mehanizmi neporecivosti

Da bi se servis neporecivosti implementirao u okruženju elektronske trgovine, sprovodi se sledeći niz aktivnosti:

1. Zahtev za servis.
2. Generisanje evidencije.
3. Transfer evidencije.
4. Verifikacija evidencije.
5. Skladištenje evidencije.

Različiti učesnici u digitalnoj komunikaciji imaju različite uloge u svakoj od navedenih faza. To zavisi od tipa neporecivosti.

Da bi se ostvarila neporecivost, učesnici moraju da se sporazumeju unapred da će se sprovoditi pomenute aktivnosti i generisati pomenuta evidencija. Zbog toga je potreban zahtev za servis neporecivosti, koji generiše jedna od strana učesnica u komunikaciji, ili treća strana od poverenja. Ovakav eksplicitan zahtev može se ponekad zameniti ugovorom koji sadrži klauzulu da se servis neporecivosti uvek koristi. Na taj način, uloga preliminarne faze servisa neporecivosti (tj. zahteva za servis) pripada licu koje zahteva servis. U opštem slučaju to je jedna od strana učesnica u komunikaciji, ali takođe može biti i ovlašćeni predstavnik. Kod servisa neporecivosti porekla, lice koje zahteva servis je primalac. Kod servisa neporecivosti prijema, lice koje zahteva servis je pošiljalac.

Generisanje evidencije je proces u kome se generišu dokumenti koji dokazuju slanje ili prijem konkretne poruke. Potencijalni negator mora da učestvuje u generisanju evidencije. Evidencija može da se šalje zajedno sa porukom ili posebno. Strana učesnica u komunikaciji koja generiše evidenciju može to da čini nezavisno ili u tom procesu može da učestvuje treća strana od poverenja. Kod servisa neporecivosti porekla, pošiljalac (ili treća strana od poverenja) mora da generiše evidenciju. Kod servisa neporecivosti prijema, primalac (ili treća strana od poverenja) mora da generiše evidenciju.

Posle prenošenja poruke koja se štiti od poricanja i generisanja odgovarajuće evidencije, evidencija se mora dostaviti strani (ili stranama) kojima je potrebna. Strane učesnice se takođe mogu sporazumeti o tome da će se evidencija dostavljati i trećoj strani od poverenja.

Posle prijema evidencije od strane učesnice koja ju je generisala, lice koje je zahtevalo servis mora da verifikuje da je primljena evidencija dovoljna da dokaže neporecivost u slučaju konflikta. Ova verifikacija se uvek sprovodi, a ne samo u slučaju konflikta. U okruženju elektronske trgovine, strane učesnice (ili treća strana od poverenja koju one odaberu) potvrđuju da je evidencija radi neporecivosti u skladu sa uspostavljenim protokolima i standardima.

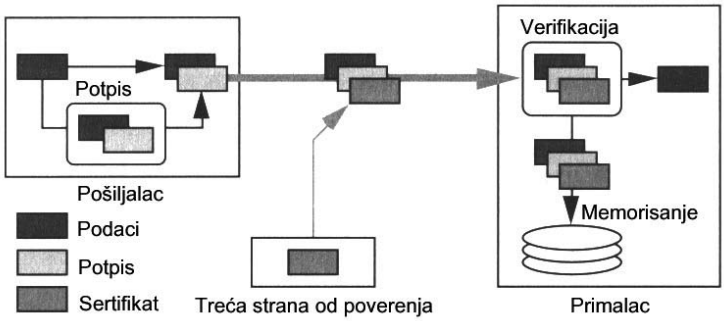
Posle verifikacije evidencije koju dostavlja strana učesnica koja ju je generisala, lice koje je zahtevalo servis mora da je uskladišti radi kasnije upotrebe. Sama ta strana

učesnica može da je skladišti, ali je bolje da to učini treća strana od poverenja. U tom slučaju se smanjuje rizik konflikta usled nepoverenja.

10.6.3 Način funkcionisanjan servisa neporecivosti

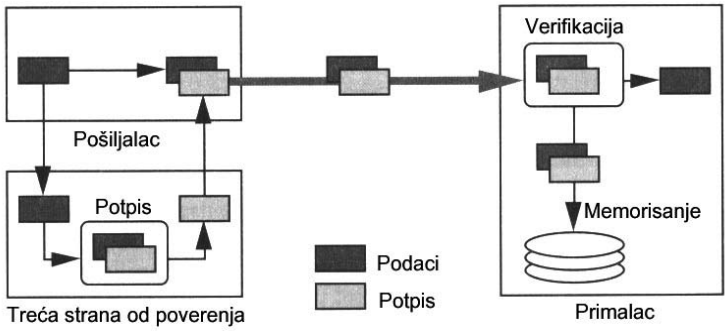
Servis neporecivosti porekla može se ostvariti na različite načine [5]:

1. Digitalni potpis pošiljaoca – Digitalni potpis pošiljaoca u tom slučaju predstavlja primarnu evidenciju. Verifikacija se sastoji od verifikacije digitalnog potpisa pošiljaoca od strane primaoca. Zatim primalac skladišti digitalni potpis pošiljaoca, zajedno sa porukom, za slučaj konflikta. Izvor konflikata može biti činjenica da je samo pošiljalac taj koji tvrdi da je njegov javni ključ originalan. Zbog toga je bolje uključiti treću stranu od poverenja koja bi verifikovala odgovarajuće digitalne potpise. Opoziv javnih ključeva takođe može biti izvor problema u procesu ostvarivanja neporecivosti. Datum i čas opoziva moraju se dostaviti svim verifikatorima evidencije. Šema servisa neporecivosti ostvarenog na opisani način prikazana je na Sl. 10.6.1.



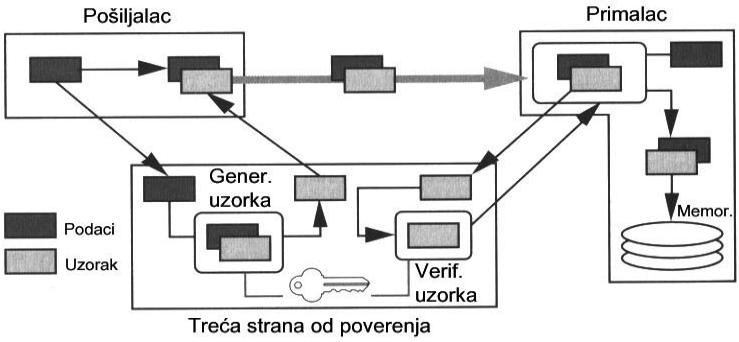
Sl. 10.6.1 – Neporecivost porekla sa digitalnim potpisom pošiljaoca

2. Digitalni potpis treće strane od poverenja – U ovom slučaju, digitalni potpis treće strane od poverenja može se koristiti sam ili zajedno sa digitalnim potpisom pošiljaoca. Ako se digitalni potpis treće strane od poverenja koristi sam, pošiljalac šalje poruku toj strani, zajedno sa podacima o identitetu i drugim eventualno potrebnim informacijama. Treća strana od poverenja autentikuje pošiljaoca i njegovu poruku i generiše dodatnu informaciju, digitalno potpisanu, koja će zajednosa porukom biti poslata primaocu. Ova informacija se može koristiti u slučaju konflikta usled poricanja. Šema servisa neporecivosti sprovedenog na opisani način prikazana je na Sl.10.6.2.



Sl. 10.6.2 – Neporecivost porekla sa digitalnim potpisom treće strane od poverenja

3. Digitalni potpis treće strane od poverenja hash funkcije poruke – U ovoj varijanti prethodnog slučaja, umesto slanja cele digitalno potpisane poruke primaocu, treća strana od poverenja digitalno potpisuje samo hash funkciju poruke i ova informacija se koristi u servisu neporecivosti.
4. Uzorak (token) treće strane od poverenja – Alternativa digitalnom potpisivanju treće strane od poverenja je njen uzorak. U ovoj šemi se koristi kriptogrtafija sa simetričnim ključevima. Umesto potpisivanja poruke, ona se štiti koristeći mehanizam provere identiteta, kao na primer MAC (message authentication code) i tajni ključ koji poznaje samo treća strana od poverenja. Informacija koja se štiti pomoću MAC-a sastoji se od poruke ili njene hash funkcije, identiteta pošiljaoca itd. Treća strana od poverenja generiše uzorak za pošiljaoca. Zatim se on šalje pošiljaocu, kao evidencija komunikacije. Očigledno je da primalac ne može sam da verifikuje tu informaciju (zato što ne zna tajni ključ) već mora da se obrati trećoj strani od poverenja. Šema servisa neporecivosti sprovedenog na opisani način prikazana je na Sl. 10.6.3.



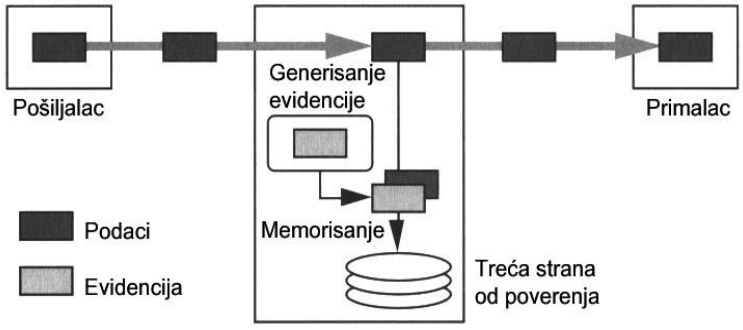
Sl. 10.6.3 – Neporecivost porekla sa uzorkom treće strane od poverenja

5. Treća strana od poverenja na komunikacionom putu – U ovom slučaju, treća strana od poverenja prosto kopira informaciju koja se prenosi između pošiljaoca i primaoca. Ono što se skladišti u memoriji treće strane od poverenja je identitet pošiljaoca, identitet primaoca i sadržaj poslate poruke. Jdna varijanta opisanog slučaja je ako treća strana od poverenja generiše digitalni potpis kao evidenciju i šalje ga, zajedno sa kopiranom porukom, primaocu (na taj način, treća strana od poverenja ne skladišti informaciju u svojoj memoriji). Prva varijanta je prikazana na Sl. 10.6.4, dok je druga varijanta prikzana na Sl.10.6.5.

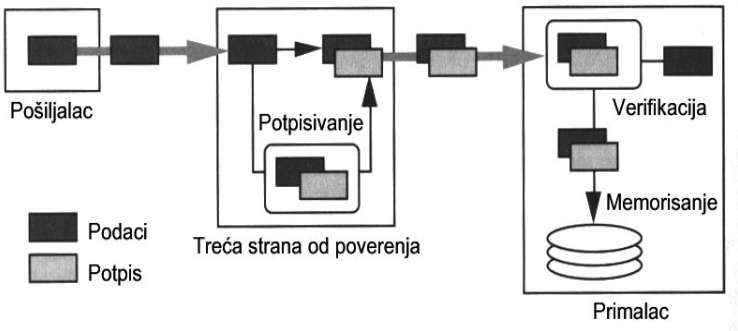
Pored opisanih mehanizama, moguće je konstruisati sistem koji kombinuje neke od njih, da bi se povećala moć servisa neporecivosti porekla.

Servis neporecivosti prijema se može ostvariti na sledeće načine:

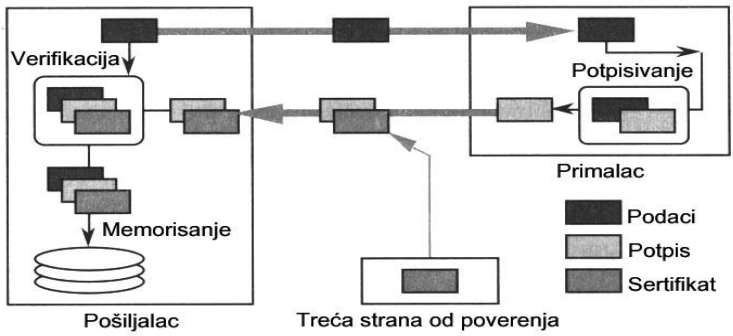
1. Potvrda prijema sa digitalnim potpisom – U ovom slučaju, primalac šalje pošiljaocu digitalno potpisanu potvrdu prijema poruke. Ova potvrda prijema sadrži kopiju onoga što je poslato ili odgovarajuću vrednost hash funkcije i druge eventualno potrebne informacije, kao na primer čas prijema. Digitalni potpis može generisati primalac ili treća strana od poverenja. Zahtevi za sertifikaciju i opoziv ključeva identični su onima opisanim kod mehanizama ostvarenja neporecivosti porekla. Ova šema je prikazana na Sl.10.6.6.



Sl. 10.6.4 – Neporecivost porekla sa trećom stranom od poverenja na komunikacionom putu – evidencija se skladišti



Sl.10.6.5 – Neporecivost porekla sa trećom stranom od poverenja na komunikacionom putu – evidencija se šalje primaocu



Sl. 10.6.6 – Neporecivost prijema sa digitalnim potpisom primaoca

2. Potvrda prijema sa uzorkom (token) – U ovom slučaju, primalac koristi uzorak koji generiše treća strana od poverenja, i koji sadrži vrednost koju ova generiše pomoću kriptografskog algoritma sa simetričnim ključevima. Jedino treća strana od poverenja je u stanju da verifikuje uzorak.
3. Dostavljač od poverenja – U ovom slučaju, treća strana od poverenja igra ulogu dostavljača poruke. Dostavljač interveniše na komunikacionom putu između pošiljaoca i primaoca i ponaša se više-manje kao primalac. Pošiljalac šalje svoju poruku dostavljaču, koji potvrđuje prijem svojim digitalnim potpisom. Ova potvrda se u opštem slučaju šalje pošiljaocu posle dostavljanja primaocu. Na taj način se onemogućava slučaj da primalac ne želi da pošalje potvrdu prijema pošiljaocu.
4. Progresivni izveštaji o prijemu – U slučajevima u kojima postoji mogućnost gubitka podataka za vreme prenosa, učesnici mogu da koriste mehanizam kod koga se provere prijema ostvaruju na više od jednog mesta na komunikacionom putu. U ovom sistemu, administratori delova komunikacione mreže (domena) su odgovorni za prolaz poruke kroz te domene.

Najčešće korišćeni mehanizam u servisu neporecivosti slanja prikazan je na Sl.10.6.6, sa digitalnim potpisom primaoca. Ovaj mehanizam se koristi u okruženjima elektronske trgovine kod kojih se poruke prenose preko treće strane, kao na primer preko provajdera elektronske pošte. Taj provajder u opštem slučaju nema interes da poriče komunikaciju, pa se zbog toga u takvom okruženju ne koriste komplikovaniji mehanizmi za ostvarenje neporecivosti.

10.7 TREĆE STRANE OD POVERENJA (TTP)

Imajući u vidu činjenicu da će organizacija koja će rešavati konflikte između učesnika u elektronskoj trgovini više verovati dokazima koje pruži treća strana od poverenja nego onim koje pruže strane u sporu, moraju se definisati karakteristike koje mora da poseduje entitet da bi se mogao smatrati trećom stranom od poverenja [6].

Treća strana od poverenja može se definisati na sledeći način:

Treća strana od poverenja je nezavisan entitet bez interesa koji doprinosi bezbednosti i pouzdanosti prenosa informacija unutar informacionog sistema.

Da bi se obezbedio servis neporecivosti, treća strana od poverenja ostvaruje ili učestvuje u ostvarivanju sledećih funkcija:

1. Sertifikacija javnih ključeva – Izdajući sertifikat javnog ključa, treća strana od poverenja potvrđuje da konkretan javni ključ odgovara konkretnom tajnom ključu, čiji je vlasnik konkretan entitet, kao i da pomenuti par ključeva važi u naznačenom periodu.
2. Potvrda identiteta – U nekim od mehanizama za ostvarivanje servisa neporecivosti, treća strana od poverenja digitalno potpisuje poruku umesto pošiljaoca. Potvrda identiteta je takođe funkcija sertifikacije javnih ključeva.
3. Generisanje vremenskog pečata (time stamp) – U opštem slučaju, vremenski pečat je sertifikat, koji generiše treća strana od poverenja, da je konkretna poruka postojala naznačenog datuma i časa. Da bi se ostvarila ova funkcija, treća strana od poverenja mora da poseduje specijalnu opremu za merenje vremena.
4. Skladištenje evidencije – Prednost učesnika u elektronskoj trgovini je u tome što treća strana od poverenja može da skladišti u svojoj memoriji evidenciju transakcija, smanjujući na taj način troškove opreme za učešće u elektronskoj trgovini. Važno je imati u vidu kvalitet memorije, pošto je informacije potrebno skladištiti u dužem vremenskom periodu.
5. Posrednik prilikom slanja – U nekim slučajevima, treća strana od poverenja može igrati ulogu dostavljača poruka. Na taj način, ona garantuje učesnicima u elektronskoj trgovini da će poruke biti uručivane bez izmena.

6. Razrešavanje konflikata – Treća strana od poverenja može igrati ulogu arbitra u konfliktima između učesnika u elektronskoj trgovini. Priroda ove funkcije je pravna, za razliku od drugih funkcija u elektronskoj trgovini.

Treća strana od poverenja mora da bude nezavisna od učesnika u elektronskoj trgovini, i eksplicitno prihvaćena od svih njih. takva organizacija može pripadati vladi, ili može biti neko preduzeće međunarodnog ili lokalnog karaktera, ili fizičko lice, kao na primer beležnik (notar) u malim okruženjima.

10.8 TRADICIONALNE BANKARSKE APLIKACIJE

Kod najvećeg broja ovakvih aplikacija mnogo je važnije perfektno identifikovati pošiljaoca i primaoca nego zaštititi podatke za vreme prenosa. Zbog toga se mnogo veća pažnja obraća servisu autentikacije nego poverljivosti. To, zajedno sa činjenicom da su poruke obično kratke, čini da se kod ovog tipa aplikacija mnogo više koriste algoritmi sa javnim ključevima, dok se blok šifre koriste samo u nekim slučajevima.

Najveći broj bezbednih bankarskih i finansijskih aplikacija se razvijaju za infrastrukturu iznajmljenih komunikacionih linija tipa X.25. Mnoge od njih su bile podložne promenama i adaptacijama da bi se mogle koristiti u drugim infrastrukturama, kao na primer X.400. Danas se uočava jasna tendencija ka korišćenju Interneta za podršku komunikacijama. Kao posledica toga, neke od aplikacija su već bile podložne promenama kako bi se adaptirale MIME formatu, koji je danas osnovni Internet standard.

10.8.1 Standard ISO 8730

To je jedan od najstarijih standarda sa najviše bezbednosnih ekstenzija namenjen međubankarskim transakcijama. Standard ISO 8730, zasnovan na standardu ANSI X9.9, koristi simetrični šifarski sistem (DES) radi autentikacije transfera, [7]. Mehanizmi distribucije ključeva su regulisani standardom ISO 8732.

U standardu ISO 8730 postoje različite opcije za obradu formatiranih podataka radi izračunavanja MAC-a. Među ovim opcijama nalazi se i mogućnost interpretacije podataka u vidu teksta ili u vidu binarnih datoteka. Ako se poruka smatra tekstom, on se može editovati uklanjajući na taj način suvišne znakove koji usporavaju rad i čine ga netransparentnim ili ostaviti takav kakav jeste. Takođe, ako se podaci smatraju tekstom, može se izabrati opcija za izračunavanje MAC-a na osnovu kompletne poruke ili na osnovu izabranih polja.

Prema standardu ISO 8730, različita polja koja čine neku međubankarsku transakciju moraju se uključiti u autentikacionu poruku. To su, između ostalih:

1. MAC – to je autentikacioni kod poruke, koji se sastoji od osam heksadecimalnih cifara.
2. DMC – to je datum izračunavanja MAC-a.
3. IDA – to je identifikator koji označava da primalac treba da koristi autentikacioni ključ.
4. MID – to je identifikator poruke. Radi se o broju koji generiše pošiljalac na osnovu DMC i IDA radi zaštite od dupliranja ili gubitka poruke.
5. Specifični elementi teksta poruke, kao što je vrednost transakcije, entiteti učesnici, korisnici, itd.

Različita polja imaju sopstvene delimitere, koji označavaju njihov početak i kraj.

10.8.2 SWIFT

SWIFT (Society for Worldwide Interbank Financial Telecommunication) nudi servis za transfer plaćanja sa različitim bezbednosnim mehanizmima, kao na primer šifrovanje na međugradskim linijama, zaštita pristupa mreži putem kodova i mogućnost šifrovanja veze između korisnika i iznajmljene mreže, [8]. Korisnici SWIFT-a obično koriste specifične produkte koje instaliraju na svojim terminalima radi identifikacije operatora.

Komunikacije se realizuju u mreži komutiranih paketa tipa X.25, a finansijske transakcije mogu koristiti različite protokole, formate i druge mere bezbednosti, kao na primer autentikaciju. SWIFT je poboljšao osnovnu bezbednost mreže dodavanjem nekih elemenata bezbednosti korisnika, kao na primer bezbedne razmene ključeva i kontrole pristupa pomoću inteligentnih kartica.

Radi realizacije operacija velikog volumena – isplate penzija, plata, informacija o upravljanju rizicima, zaštite stanja računa i drugih, SWIFT je kreirao međubankarski prenos datoteka (IFT) koji radi u okruženju X.400. Za transfer datoteka se koristi protokol pIFT, unutar poruka X.400, koji sadrži bezbednosno zaglavlje sa uzorkom ("token") (zasnovano na X.509). Bezbednosni servisi su: integritet sadržaja pIFT, autentikacija originalne poruke i poverljivost. Mogu se koristiti različiti algoritmi sa simetričnim ili asimetričnim ključevima za generisanje uzorka od strane pošiljaoca, koji sadrži identifikator odabranog algoritma. Izbor ključeva i njihova distribucija ne moraju da zavise od SWIFT-a.

Kako se razvijaju produkti EDI i za X.25 i za X.400, EDI kao i EDIFACT postepeno zamenjuju originalni format koji je dizajnirao SWIFT.

10.8.3 ETEBAC 5

Protokol ETEBAC 5 je dizajn Comité Fran□ais d´Organisation et de Normalisation Bancaires (CFONB) namenjen korišćenju u francuskom bankarstvu, koji omogućava realizaciju

operacija iz izvesnog opsega između finansijskih institucija i njihovih klijenata na siguran način, [9].

ETEBAC 5 koristi protokol za transfer datoteka koji se naziva PeSIT i komunikacioni kanal X.25. Prihvata kriptografske algoritme sa simetričnim ili asimetričnim ključem, DES i RSA, respektivno.

Među bezbednosnim servisima koje nudi ETEBAC 5 nalazi se međusobna autentikacija banke i klijenta, integritet podataka zaštićen MAC-om, međusobna neporecivost i poverljivost podataka koji se štite DES-om (opcioni servis). ETEBAC 5 zavisi od ustanove za sertifikaciju, koja izdaje sertifikate tipa X.509 korisnicima kojima je potreban javni ključ.

Razlikuju se dva funkcionalna nivoa prilikom transfera datoteka, od kojih svaki koristi različite ključeve. Zadatak jednog nivoa je zaštita sadržaja datoteka koje se razmenjuju, dok drugi nivo odgovoran za bezbednost prilikom uspostavljanja veze.

ETEBAC 5 sadrži mnoge elemente koji omogućavaju veliku fleksibilnost i bezbednost njegovih servisa. Na primer, ne potpisuje se samo sadržaj datoteke, već takođe i MAC identifikatora datoteke. ETEBAC 5 je bio prvi standard koji je koristio RSA kao sistem sa javnim ključevima.

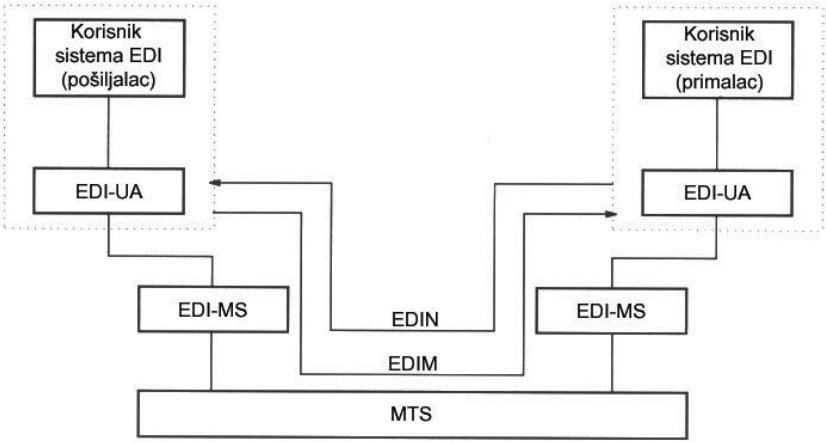
10.9 ELECTRONIC DATA INTERCHANGE (EDI)

Aplikacija poznata pod imenom elektronska razmena podataka (EDI) takođe poseduje dosta dobro definisane i normalizovane bezbednosne servise [10]. Prilikom njegovog korišćenja u komercijalnim transakcijama prvenstveno se zahteva servis autentikacije.

ITU je izradio dva standarda: preporuke F.435 i X.435, koje omogućavaju upotrebu EDI u sistemima za razmenu poruka tipa X.400. Preporuka F.435 definiše servise za razmenu poruka EDI, a X.435 definiše sisteme za razmenu poruka EDI, tj. način rada servisa opisanih u F.435.

EDI poruke (EDIM) sastoje se od zaglavlja i tela koji zajedno čine polje sadržaja poruke tipa X.400. U zaglavlju se pojavljuju brojna polja koja definišu identifikaciju i vrste obrade kroz koje mora da prođe poruka, ali samo neka od tih polja imaju veze sa bezbednošću. U telu poruke mogu da se pojave polja tipa EDIFACT (standard ISO 9735, [11]) ili tipa ANSI X12, [12].

EDI notifikacija (EDIN) je poruka povezana sa originalnom porukom sa kojom ima zajednički niz polja, iza kojih se nalaze polja koja označavaju tip notifikacije. EDI notifikacije omogućavaju potvrdu prijema poruke na nivou aplikacije, a ne samo njeno dostavljanje. Na Sl. 10.9.1 može se videti način transfera EDI poruka i notifikacija.



Sl. 10.9.1 – Funkcionisanje EDI poruka i notifikacija

F.435 i X.435 uvode dodatne bezbednosne elemente u odnosu na one već prisutne u X.400, radi garancije autentičnosti i neporecivosti kako poruka tako i notifikacija. Pošiljalac EDI poruke može zahtevati servis potvrde/neporecivosti aktiviranjem odgovarajućih bita u polju zahteva unutar notifikacije koje se nalazi u zaglavlju.

Upotreba EDI na Internetu definisana je u RFC 1865, [13]. U MIME su uključene tri različite vrste informacija radi prepoznavanja formata koji koriste EDI poruke:

1. Jedna vrsta informacija MIME radi kompatibilnosti sa razmenom EDI poruka u formatu ANSI X.12.
2. Jedna vrsta informacija MIME radi kompatibilnosti sa razmenom EDI poruka u formatu EDIFACT.
3. Jedna vrsta informacija MIME radi kompatibilnosti sa razmenom EDI poruka u formatu različitom i od ANSI X.12 i od EDIFACT i o kome moraju unapred da se sporazumeju pošiljalac i primalac.

Prilikom realizacije prenosa EDI poruka putem Interneta mogu se koristiti bezbednosni mehanizmi koje nudi S/MIME kao dodatni servisi globalne bezbednosti strukture poruke.

Iako se X.400 koristi za kompletnu zaštitu razmene EDI podataka, nije struktura poruka+notifikacija jedina koja može da se koristi. Razmena podataka se sastoji od razmene poruka i funkcionalnih grupa – grupa sličnih poruka – sve sa istom destinacijom, ali nije svima potrebna zaštita. X.435 nije u stanju da realizuje selektivnu bezbednost.

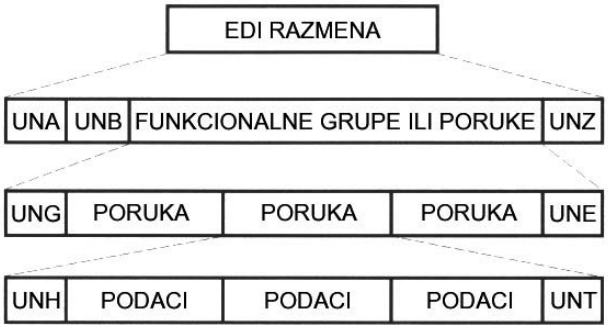
Zbog toga, radi zaštite razmene podataka i pođedinica podataka uvedena je zaštita unutar same EDI strukture korišćenjem izvesnih indikatora. Da bi se regulisale operacije

ovog tipa pojavili su se različiti standardi, između kojih treba pomenuti serijuANSI X12 i naročito EDIFACT.

Struktura EDIFACT poruke može se videti na Sl.10.9.2. Vidi se da svaki deo sadrži delimitere unutar zaglavlja (UNA, UNB, UNG, UNH) i na kraju (UNZ, UNE, UNT).

Delimiteri unutar zaglavlja identifikuju i specificiraju razmenu i funkcionalnu grupu ili poruku, dok se delimiteri na kraju koriste radi realizacije provera.

Program TEDIS [14], Evropske komisije realizuje bezbednosne servise EDIFACT-a, uglavnom radi kontrole autentičnosti poruka i na nivoima razmene koji se zasnivaju na asimetričnim ključevima.



Sl. 10.9.2 - Struktura EDI poruke

10.10 SISTEMI ZA ELEKTRONSKO PLAĆANJE

Elektronska trgovina uopšte, kao i onaj njen deo koji se realizuje na Internetu, zavise od raspoloživosti i široke primene sistema za elektronsko plaćanje. Jezgro sistema za elektronsko plaćanje sastoji se od različitih protokola za plaćanje. Ovi protokoli mogu biti ugrađeni u pretraživače (HTTP), klijente elektronske pošte (SMTP) ili u druge programe koji koriste neke protokole sa specifičnom primenom.

Iako danas ovi sistemi funkcionišu odvojeno jedan od drugog, tendencija je da oni mogu međusobno da komuniciraju.

10.10.1 Elektronski novac

10.10.1.1 Osnovni pojmovi

Svrha elektronskog novca (e-cash) je da obezbedi elektronski sistem koji je ekvivalentan fizičkom novcu na koji smo navikli. Elementi koji čine ovaj sistem su sledeći:

1. Banka koja nudi servis, tj. koja izdaje elektronski novac.
2. Lice – klijent – koje će trošiti novac koji izdaje banka.
3. Lice – prodavac – koje će primiti novac od klijenta.
4. Banka koja će primiti novac od prodavca.

Elektronska transakcija sastoji se od tri različite i nezavisne operacije:

1. Klijent podnosi zahtev za prenos sredstava sa njegovog računa u banci, putem servisa e-cash. Banka mu izdaje zahtevani iznos, a klijent ga memoriše na svom disku ili na nekoj inteligentnoj kartici. Na taj način klijent dolazi do elektronskog novca.
2. Kada se elektronski novac jednom nađe u posedu klijenta, on može da realizuje svoje kupovine. Klijent će prebaciti na račun prodavca iznos koji odgovara vrednosti kupljene robe.
3. Prodavac, dobivši elektronski novac koji je platio klijent, mora da ga prebaci u banku koja izdaje elektronski novac i taj novac dolazi na račun prodavca u toj banci.

Postoje neka svojstva koja elektronski novac mora da zadovolji. Na prvom mestu, mora biti potpuno nezavisan od platforme koja se koristi i od mesta na kome se koristi.

Elektronski novac mora zadržati osobinu anonimnosti, što je karakteristika i uobičajenog novca, što znači da se ne može doći do informacije o njegovim prethodnim vlasnicima. Na taj način, elektronski novac mora da prelazi od jednog do drugog entiteta bez ostavljanja traga (u tehničkom smislu) o prethodnom vlasniku. Međutim, moraju se preduzeti mere da klijent ne može ponovo da koristi već potrošeni novac.

Osobina anonimnosti je veoma kontraverzna, pošto bi mogla da bude zloupotrebljena od strane falsifikatora ili "perača" ilegalno stečenog novca. Zato su sistemi koji se razvijaju "skoro" anonimni, što znači da se do identiteta klijenta može doći pod izvesnim uslovima (na primer, postupajući po sudskom nalogu).

Skladištenje elektronskog novca na disku ili na inteligentnoj kartici mora biti bezbedno.

10.10.1.2 Primeri: DigiCash, NetCash, CyberCash

1982. godine David Chaum je razvio mehanizam slepog potpisa sa algoritmom RSA radi davanja osobine anonimnosti elektronskom novcu, i osnovao preduzeće DigiCash radi komercijalizacije ove šeme pod imenom Ecash, [15]. 1995. godine pojavila se jedna banka u SAD koja je prva ponudila ovaj servis.

U sistemu Ecash, digitalni apoeni se lokalno skladište u sistemu klijenta. Ovi digitalni apoeni se mogu šifrovati koristeći tajni ključ izveden iz lozinke, ili se mogu koristiti inteligentne kartice.

Pre prihvatanja apoena, prodavac mora da ispita njegovu autentičnost i integritet pomoću odgovarajućeg javnog ključa banke koja izdaje apoene. Zatim mora da verifikuje on-line da li je apoen prethodno korišćen ili ne od strane istog korisnika. Jedan apoen može biti korišćen samo jednom. Da bi se to postiglo, banka dodeljuje serijske brojeve apoenima da bi mogla da ih identifikuje i da odbaci apoen koji neko želi ponovo da iskoristi. Ideja anonimnosti u sistemu Ecash bila je studiozno proučavana u okviru projekta pod nazivom Conditional Access for Europe, poznatog kao CAFE, [16]. Rezultati istraživanja pokazuju da se ne može uvek realizovati on-line provera apoena i da se sistem bolje ponaša ako se provera apoena vrši off-line.

Da bi se pomoću off-line provera onemogućila višestruka upotreba apoena, definisana su izvesna rešenja. Jedno od njih je korišćenje složenih matematičkih algoritama koji omogućavaju da se dođe do identiteta vlasnika, na taj način što se deo informacija o vlasniku prenosi istovremeno sa plaćanjem. Ova informacija sama za sebe ne otkriva identitet, već mora da se kombinuje sa drugim delom identifikacije.

Sistem za elektronsko plaćanje NetCash razvio je Information Sciences Institute, University of Southern California [17]. Koristi višeslojnu autentikaciju, kao i poboljšani sistem provera višestrukog korišćenja apoena.

U okviru višeslojnog protokola za autentikaciju, svako ko želi da uspostavi novčani server ("currency server") mora da dobije dozvolu od državne agencije kao na primer od Federalnih rezervi SAD. Novi novčani server počinje da funkcioniše generisanjem para ključeva i slanjem javnog ključa agenciji. Zatim agencija generiše sertifikat, potpisan pomoću njenog tajnog ključa, za konkretan server. Ovaj sertifikat sadrži javni ključ servera i jedinstveni identifikacioni broj koji odgovara serveru. Pomenuti sertifikat služi kao garancija serveru, koji sada može da počne da izdaje apoene. Apoeni sadrže broj servera, serijski broj apoena i vrednost i potpisani su pomoću privatnog ključa servera. Pored toga, sadrže referencu na sertifikat agencije, koji omogućava svakom korisniku da ga proveri kad god želi.

Metod koji se koristi radi provere da li neko pokušava da više puta iskoristi isti apoen suprotan je od onog koji koristi sistem DigiCash. U sistemu NetCash, serijski broj svakog apoena se skladišti u momentu emitovanja. Kada se jedan apoen nađe na proveri na serveru, proverava se da li se nalazi na listi emitovanih apoena. Ako se nalazi na toj listi,

radi se o validnom apoenu i njegov serijski broj se briše sa liste. Međutim, ako se serijski broj apoena ne nalazi na listi, uzrok tome može biti pokušaj klijenta da dva puta iskoristi isti apoen, ili da je apoen generisan od strane drugog servera (tj. da je falsifikovan). U svakom slučaju, takav apoen nije validan i na taj način je detektovan problem.

Koji od sistema, DigiCash ili NetCash, je efikasniji zavisi od opticaja apoena. Ako je broj validnih apoena u opticaju veći od broja potrošenih validnih apoena u nekom vremenskom periodu, sistem DigiCash je efikasniji. U protivnom, sistem NetCash je efikasniji. Ali sistem NetCash je bolji od sistema DigiCash ako se razmatra mogućnost višestruke upotrebe jednog apoena.

Na žalost, u sistemu NetCash novčani server može da dođe do informacije o identitetu vlasnika apoena. To znači da u ovom sistemu anonimnost nije zagarantovana.

Kompanija CyberCash Inc. nudi neke sisteme za elektronsko plaćanje kod kojih se koriste protokoli slični onima koji se koriste u sistemima plaćanja kreditnim karticama [18]. Sistem CiberCash povezuje softver za prodavce sa softverom za server CyberCash, služeći kao interfejs između prodavca na Internetu i bezbedne bankarske mreže. Transakcija u ovom sistemu se sastoji od sledećih koraka:

1. Klijent koji će nešto da kupi po ponuđenoj ceni sporazume se o tome sa prodavcem. Zatim primi profakturu sa prodavčevog servera.
2. Klijent koristi softver CyberCash Wallet radi plaćanja. Ovaj program generiše dokument o plaćanju koji se šalje prodavcu u šifrovanom obliku.
3. Prodavac digitalno potpisuje dokument primljen od strane klijenta i šalje ga CyberCash serveru.
4. CyberCash server koristi specifičan softver radi dešifrovanja primljenog dokumenta, menja format pomenute poruke i šalje ga u banku prodavca.
5. Banka prodavca šalje pomenuti dokument u banku kupca, u kojoj se transakcija potvrđuje ili odbija.
6. Izveštaj o transakciji se šalje CyberCash serveru.
7. CyberCash server šalje poruku prodavcu, u kojoj ga obaveštava o tome da li se transakcija prihvata ili odbija.

Koraci 1, 2, 3 i 7 se odvijaju na Internetu i koriste kombinaciju javnih ključeva i simetričnih kriptografskih algoritama. Koraci 4 i 6 se idvijaju na specifičnim linijama. Korak 5 se odvija u već postojećoj finansijskoj mreži. Cela transakcija se završava u roku od 15-20 sekundi.

Sistem CyberCash nije ekonomičan za mikro plaćanja, zato što se koristi okruženje kreditnih kartica. Ne koriste se pravi apoeni. Iznos se ne nalazi na računaru klijenta, već unutar već postojeće finansijske mreže. Prednost ovoga je u tome da kvar na računaru klijenta ne utiče na realni novac. Međutim, sistem CyberCash nije anoniman i svi podaci o transakciji se skladište u finansijskoj mreži.

10.10.2 Kreditne kartice

Postoje različiti bezbednosni protokoli za realizaciju plaćanja pomoću kreditnih kartica prilikom elektronske kupovine, kao na primer iKP, koji je razvio IBM, i protokoli SET i CCPS, koje su zajedno razvili Visa i MasterCard. Protokol SET je najraširenij od svih pomenutih.

10.10.2.1 iKP

IBM Research Division je razvio familiju protokola za bezbedno plaćanje, pod imenom iKP, zasnovanu na ideji koju su objavili Mihir Bellare et. al. 1995. godine. Pomenuta familija protokola je namenjena za korišćenje unutar svakog pretraživača i/ili servera na bilo kojoj platformi. Prvi prototip sistema bio je namenjen za upotrebu u kreditnim karticama, ali kako je njegova unutrašnja konstrukcija fleksibilna, može se koristiti i u drugim sistemima za plaćanje. Prvi prototip je bio izrađen u potpunosti softverski, zato što današnji računari ne koriste inteligentne kartice ni druge vrste specijalizovanog hardvera, ali postoji mogućnost modifikacije sistema radi upotrebe pomenutog hardvera.

Tehnologija iKP zasnovana je na sistemu RSA sa javnim ključevima. U zavisnosti od zahteva, transakcija plaćanja može da koristi jedan, dva ili tri javna ključa. U svakom slučaju, banka koja je u vezi sa ovim transakcijama poseduje par javni ključ – tajni ključ radi prijema poverljive informacije kao na primer broja kreditne kartice, digitalnih potpisa radi autorizacije itd. U mnogim slučajevima, prodavac takođe poseduje par javni ključ – tajni ključ radi prijema poverljivih informacija i potpisivanja zahteva za plaćanje i potvrda kupovine. U nekim slučajevima, čak i klijent može imati svoj sopstveni par javni ključ – tajni ključ radi digitalnog potpisivanja transakcija plaćanja. U svakom slučaju, klijent ima svoj sopstveni PIN (Personal Identification Number) radi potvrde autorizacije plaćanja.

Pretpostavlja se da su se, pre poziva iKP, klijent i prodavac sporazumeli o detaljima kupovine (profaktura, valuta, cena i način plaćanja). Prodavac može da istovremeno kombinuje autorizaciju sa realizacijom plaćanja, ili može da realizuje plaćanje kasnije. Prodavac šalje zahtev za plaćanje banci klijenta koja mu odgovara šaljući mu informaciju o mogućnosti plaćanja. Ako je sve u redu, prodavac šalje klijentu potvrdu o tome. Plaćanje se takođe može poništiti, ako se ne može realizovati zbog nekog razloga (tehničke ili bilo koje druge prirode).

Informacija koja se prenosi između banke i prodavca, kao i podaci o autentikaciji prodavca, šifruju se.

10.10.2.2 SET

Prva verzija protokola SET bila je objavljena u februaru 1996. godine, a druga u junu iste godine. Ona se sastoji od tri dela: Knjiga 1, gde se opisuje tip trgovine; Knjiga 2, koja je vodič za programere, i Knjiga 3, koja sadrži formalnu definiciju protokola.

Elementi koji čine okruženje SET su sledeći:

1. Centar za emitovanje korisničkih kartica (Issuer). To je finansijska institucija koja emituje kartice.
2. Korisnik kartice (Cardholder). To je vlasnik bankarske kartice autorizovan od strane emisionog centra.
3. Trgovac (Merchant). To je prodavac koji prihvata elektronsko plaćanje.
4. Finansijski entitet na usluzi trgovcima (Adquirer). To je finansijska institucija koja daje podršku trgovcima u procesu izvršenja transakcija putem bankarskih transakcija.
5. Put plaćanja (Payment gateway). To je sistem koji prodavcima omogućava on-line komercijalne servise.
6. Ustanove za sertifikaciju (Certification authorities). To su centri za sertifikaciju javnih ključeva ostalih elemenata sistema.

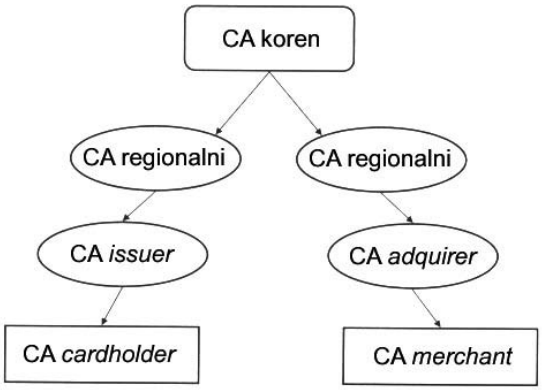
Transakciju plaćanja čine sledeći koraci:

1. kada korisnik želi da realizuje kupovinu, šalje prodavcu on-line instrukciju za plaćanje.
2. Trgovac komunicira on-line sa svojim finansijskim entitetom, preko puta plaćanja, da bi autorizovao transakciju. U opštem slučaju, trgovac prosto šalje instrukciju za plaćanje koju je primio od klijenta.
3. Finansijski entitet trgovca skladišti informaciju i može da zahteva transakciju od emisionog centra.
4. Na kraju, ako je sve u redu, niz potvrda (emisionog centra finansijskom entitetu, finansijskog entiteta trgovcu i trgovca klijentu) omogućava vlasniku kartice da realizuje kupovinu.

U okruženju SET, upotreba asimetričnih ključeva omogućava sledeće funkcije:

1. Šifrovanje instrukcija za plaćanje radi zaštite broja kartice.
2. Autentikacija vlasnika kartice kod trgovca i finansijskog entiteta radi zaštite vlasnika od krađe kartice. Ovaj servis je opcija.
3. Autentikacija trgovca kod klijenta i kod finansijskog entiteta kao zaštita od suplantacije.
4. Autentikacija finansijskih entiteta kod vlasnika kartica i trgovaca, radi onemogućavanja napadaču da putem suplantacije doće do osetljivih podataka sadržanih u instrukcijama za plaćanje.
5. Zaštita integriteta podataka koji se prenose.

Javni ključevi su hijerarhijski uređeni kao na Sl.10.10.1. Postoji glavna ustanova – vrhovni CA – koja sertifikuje CA ustanova za emisiju kreditnih kartica. CA svake ustanove za emisiju kartica može da bude odgovorna za različita geopolitička okruženja i da sertifikuje odgovarajuće CA iz svakog od tih okruženja, a one opet sertifikuju druge CA koje na kraju sertifikuju korisnike.



Sl. 10.10.1 – Hijerarhija sertifikacije u protokolu SET

10.10.2.3 CCPS

Sistem kreditnih kartica CCPS (Chip Card Payment System) koji je razvila kompanija VISA koristi kriptografiju sa javnim ključevima radi autorizacije plaćanja i tehnologiju Smart Card radi konstrukcije kartica. detalji sistema nisu objavljeni, osim činjenice da je algoritam sa javnim ključevima koji se koristi RSA, i da dužina javnih ključeva može biti 768, 896 ili 1024 bita. Javni ključevi su objavljeni na Web serveru kompanije VISA.

10.10.3 Mikro plaćanja

Vrlo važan faktor koji treba uzeti u obzir prilikom vrednovanja sistema za plaćanje su dodatni troškovi koje unose bankarski servisi za različite transakcije. u vezi sa ovom idejom pojavljuju se sistemi za mikro plaćanje, namenjeni za obradu velikog broja operacija prenosa malih iznosa, koji takva plaćanja u najvećem broju slučajeva grupišu radi realizacije jedne jedine transakcije.

Neke od najpoznatijih implementacija su:

1. Millicent, kompanije DEC.
2. PayWord i MicroMint, koje su razvili Rivest y Shamir.
3. CyberCoin, kompanije CyberCash.

Protokol Millicent, koji je uvela Digital Equipment Corporation (DEC) 1996. godine razvijen je kao sistem za obradu elektronskih plaćanja malih vrednosti od 0.1 centa do 5 dolara [19]. Koristi entitete "broker" i "scrip". Scrip sadrži vrednost plaćanja. Ako je ova vrednost veća od vrednosti kupovine, prodavac ("merchant") vraća razliku klijentu u obliku novog scrip-a.

Prodavci izdaju scrip-ove koji se mogu koristiti samo u njihovim prodavnicama. Svaki scrip ima svoj serijski broj i digitalno je potpisan od strane prodavca. Na taj način prodavac može lako da proveri validnost scrip-a, kao i to da li je prethodno već korišćen. Brokeri kupuju scrip-ove sistema Millicent u velikim količinama, i kasnije ih preprodaju individualnim klijentima.

U ovom sistemu nema potrebe za centralnim serverom za validaciju scrip-ova, zato što ih izdaju sami prodavci. Ovo smanjuje interne troškove sistema. Sistemu Millicent takođe nije potrebna vrlo jaka kriptozaštita, zato što obrađuje samo male sume novca.

10.11 LITERATURA

[1] PKI Practices and Policy Framework Draft, ANSI X9.79 standard

[2] NIST PKI Project Team, *Certificate Issuing and Management Components Protection Profile*, 2001

[3] C. Kaufman, R. Perlman, and M. Speciner, *Network Security*, second edition, Prentice Hall, 2002.

[4] http://www.itu.int/rec/T-REC-X.509/

[5] W. Ford and M.S. Baum, "Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption ", 2nd Ed., Prentice Hall, 2001.

[6] M.Milosavljević, G.Grubor, "Osnove bezbednosti i zaštite informacionih sistema", Univerzitet Singidunum, Beograd, 2006.

[7] http://www.iso.org/iso/home.htm

[8] http://www.swift.com/

[9] http://www.etebac.com/US/default.htm

[10] M. Kantor, J. H. Burrows (1996-04-29). "Electronic Data Interchange (EDI)", National Institute of Standards and Technology. http://www.itl.nist.gov/fipspubs/fip161-2.htm

[11] http://www.iso.org/iso/catalogue_detail.htm?csnumber=35033

[12] http://www.x12.org/

[13] http://www.ietf.org/rfc/rfc1865.txt

[14] http://www.tedis-wv.org/

[15] D. Chaum, "Blind signatures for untraceable payments", *Advances in Cryptology — Crypto '82*, Springer-Verlag , pp,199-203, 1983.

[16] http://www.semper.org/sirene/projects/cafe/index.html

[17] http://www.netcash.com/

[18] http://www.cybercash.com

[19] S. Glassman, M. Manasse, M. Abadi, P. Gauthier, P. Sobalvarro, "The Millicent Protocol for Inexpensive Electronic Commerce", *In Proceedings of Fourth International World Wide Web Conference,* Boston, USA, 1995. http://www.w3.org/Conferences/WWW4/Papers/246/

Odlukom Senata Univerziteta "Singidunum", Beograd, broj 636/08 od 12.06.2008, ovaj udžbenik je odobren kao osnovno nastavno sredstvo na studijskim programima koji se realizuju na integrisanim studijama Univerziteta "Singidunum".

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

004.738.5:339(075.8)

МИЛОСАВЉЕВИЋ, Милан, 1952-
Elektronska trgovina / Milan Milosavljević, Vladislav Miškovic. - 1. izd. - Beograd : Univerzitet Singidunum, 2011 (Loznica : Mladost grup). - X, 262 str. : ilustr. ; 25 cm

Tiraž 500. - Bibliografija uz svako poglavlje.

ISBN 978-86-7912-338-1
1. Мишковиц, Владислав, 1957- [аутор]
a) Електронска трговина b) Електронско пословање
COBISS.SR-ID 181880844